Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns

(利用者の行動パターンの検知を通じた機密情報とコミュニケーションの内部統制に関する研究)

By

SUCHINTHI FERNANDO

Dissertation

Submitted in partial fulfilment of the requirements for the degree

DOCTOR OF ENGINEERING

Graduate School of Information Science and Control Engineering

Nagaoka University of Technology

Nagaoka, Niigata, Japan

August 2014

Declaration

I hereby declare that this dissertation is entirely the result of my own work, except where otherwise indicated. I have used only the resources given in the list of references.

Date	Student's Signature
2014/6/18	FERNANDO S.A.
	(Suchinthi Fernando)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Engineering.

Date	Supervisor's Signature
June 16, 2014	湯川 高志
	(Prof. Takashi Yukawa)

The dissertation titled

Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns

by

Suchinthi Fernando

is reviewed and approved by:

Supervisor:

Prof. Takashi Yukawa

Co-Supervisors:

Prof. Tatsuo Asai

Prof. Yoshiki Mikami

Prof. Yoshimi Fukumura

Prof. Katsuyuki Yamazaki

Nagaoka University of Technology

August 2014

Dedication

This dissertation is dedicated to my loving family…

Acknowledgments

I wish to extend my deepest gratitude to my advisor, Prof. Takashi Yukawa, for his guidance, valuable suggestions and constant supervision throughout my research, without which, the successful completion of this study would not have been possible.

I would also like to thank my co-supervisor Prof. (Emeritus) Tatsuo Asai for providing me with guidance and encouragement throughout the course of my degree.

My gratitude is also extended to Prof. Yoshiki Mikami, Prof. Yoshimi Fukumura, and Prof. Katsuyuki Yamazaki for their support, guidance and valuable comments, which enabled me to improve my research and this dissertation.

Special thanks also go out to all the respondents who helped evaluate the usability and performance of the system implemented through this research.

Further, I also wish to thank the members of my laboratory for their support and encouragement at all times.

Finally, I would like to express my warmest and greatest appreciation to my family and friends for their constant support, guidance and encouragement.

Abstract

The focus of information security has shifted from being “technology-oriented” to being “management-oriented” during the past decade since most identified information security breaches occur because of human errors. It is also observed that most information security attacks occur from the inside or with the involvement of an insider. Even though effective information security uses physical, technical, and operational controls, where operational controls concern the conduct of employees with regard to information security, the adherence of employees of an organization to its policies is automatically assumed instead of ensured. Thus, despite the overall understanding that the human factor should be taken into consideration in information security management (ISM), most security solutions available today still rely on purely technical measures to enforce information security. Yet, people may easily bypass technological controls and restrictions by revealing their authentication information to others.

This research addresses the problem of improper sharing of information by authorized insiders with outsiders or unauthorized insiders, and proposes a managerial solution, which employs a mix of technological and social methods and techniques to achieve internal control of information and communication within an organization. As human behaviour can be categorized, this research proposes the concept of behavioural profiling, a method similar to criminal profiling, in order to predict behavioural patterns of employees. The levels of observance of secure practices by the organization’s employees are monitored through the automatic detection of their cyber activity by the security system and personal observance of their non-cyber activity by their managers and the security personnel. Human resource managers conduct background checks on employees to obtain their background information, and all this information is combined together in order to create employee security behavioural profiles by categorizing behavioural patterns, and thus help in identifying employees whose actions could potentially lead to ISM problems and information security infractions. The solution further entails determining and scheduling the level and type of security education and training to be given to each user. By employing socio-technological information gathering techniques and methods to provide a managerial solution to this human-related problem of information security, the concept proposed through this research overcomes the

weaknesses of a purely technological solution.

The system implemented to prove the feasibility of the proposed concept computes cyber activity of users, allows non-cyber activity and background information to be inputted to the system by managers and security personnel, and by human resource managers, respectively, then compiles security behavioural profiles and determines the level of security education and training required by each of the employees, and presents the behavioural profiles and security education and training schedules in summarized, detailed and graphical forms. It also allows the information security officer to view behaviour concerning cyber activity, non-cyber activity, and background information, separately and thereby recognize if the managers and security personnel who personally observe the employees' non-cyber activity display any personal bias towards the employees, and thus use his or her own personal judgement. Further by allowing the information security officer to configure the security behavioural rules to be aligned with the business objectives of the organization, this system can be tailor-made to suit the specific requirements of the organization.

The results of the testing of this implemented system show that the system can compute users' cyber activity as expected and that the developed profiles can effectively predict security behavioural flaws leading to information security infractions. The results of the usability evaluation performed on this system implementation prove that the system provides suggestions concerning employees' security behaviour in a convenient and user-friendly fashion to enable faster decision-making by information security officers and security managers.

Keywords: information security, insider threat, human behaviour, profiling, personality type, social, technological

Contents

List of Figures

List of Tables

Chapter 1

Overview

Chapter 1

Overview

1.1 Introduction

The concept of information security began with its focus revolving around technological aspects (Bishop, 2003), (Harris, 2004), such as cryptography, secure networking protocols, ethical hacking, digital forensics, etc. With the realization that security was a process rather than an end result, came the addition of secure software development. The human aspect pertaining to information security was recognized during the past couple of decades (Asai, 2007) with international standards such as ISO/IEC 270001 (2005) and the COSO framework (1994) emphasizing the importance of taking human resource security into consideration when managing information security. Thus, the role of information security has now become more management-oriented than technology-oriented, and this change is defined by Lacey (2009) as "The shifting focus of information security" (Lacey, 2009).

Vroom and von Solms (2003) explain that physical, technical and operational controls are used to carry out effective information security, where the operational controls are those that concern the behaviour and actions of the employee with regard to information security. As the conduct of the employee within the organization plays an increasingly vital role in securing information, operational controls are considered extremely important. They state that: "In order to regulate this behaviour and conform to the objectives of the company, the employees of the organization need strict and proper guidelines. These guidelines are set out in the information security policies of the organization, detailing the procedures, rules and regulations that need to be followed by the employees in order to preserve the integrity and confidentiality of company information." (Vroom & von Solms, 2003). Yet, they argue that even though information systems security auditing has been introduced to ensure that these policies, procedures and regulations are effective, auditing is not performed on the employees who actually follow the operational controls that are prescribed. Instead, "it is simply assumed that the employee will adhere to these audited policies" (Vroom & von Solms,

2003). Thus, it can be seen that despite the overall understanding that the human factor should be taken into consideration in information security management (ISM), most security solutions available today still rely on purely technical measures to enforce information security. Yet, people may easily bypass technological controls and restrictions such as access control by revealing their authentication information to others.

In order to succeed in business, it is mandatory to ensure that access to information is strictly limited to the personnel who need to know it in order to perform their assigned tasks (Schweitzer, 1996). Yet, as Bean (2008) states, most identified information security breaches occur because of human errors, resulting from the lack of proper knowledge and training, ignorance, and failure to follow procedures. Some of the most common information security problems of today include unintentional sharing of confidential information (Asai & Fernando, 2011_a), (Asai, Fernando & Castillo, 2011), (Fernando & Asai, 2011_a), (Fernando & Asai, 2011_b), not understanding or valuing ISM rules (Asai & Fernando, 2011_b), (Fernando & Asai, 2011_a), (Insight Express, 2008), and using any means to reach goals (Fernando & Asai, 2011_b). People's beliefs and expectations may lead to mistakes and misjudgements of risks (Pronin, 2006). Thus, being the weakest link in the chain of security, people may unintentionally reveal confidential information to others. Schneier (2008) explains how the perception of security diverges from its reality and how people feel secure as long as there is no visible threat. This human weakness is exploited in most present-day attacks, which require a human element to be completed successfully (Williams, 2011). These attacks may come in the forms of social engineering, spear phishing or collusion from an insider, where people are tricked into revealing confidential information to others.

1.2 Background

1.2.1 External Threat Detection vs. Insider Threat Detection

Studies concerning Intrusion Detection Systems (IDSs) prevail in the field of information security. Yet, according to Lynch (2006), 60%-70% of attacks originate from the inside with the involvement of "trusted" folks. Grimes (2010) further states that, with the inclusion of users with non-malicious intent, the percentage of insiders wittingly or unwittingly involved in an attack reaches at least 80%. Additionally, internal attacks are also considered to be more

costly than external attacks. Thus, this research focuses on intentional or unintentional information sharing by authorized insiders having access rights to business information, with outsiders or other insiders not authorized to access that information. In order to differentiate between intrusion detection and detection of internal threats, the following subsections study these two areas in detail.

1.2.1.1 Intrusion Detection

Ning, Jajodia and Wang (2003) define an intrusion in an information system as "an activity that violates the security policy of the system". They further explain that intrusion detection is the process to identify intrusions based on the belief that the intruder's behaviour will be noticeably different from that of a legitimate user and that many unauthorized actions will be detectable. IDSs are a second line of defence and are usually deployed along with other preventive security mechanisms such as access control and authentication (Ning, et al., 2003).

The two basic types of intrusion detection techniques are:

Anomaly detection: detecting actions that significantly deviate from the normal behaviour of a subject, user or system

Misuse detection: catches intrusions by detecting actions conforming to the patterns or characteristics of known attacks or system vulnerabilities (attack signatures)

Ning, et al. (2003) classify IDSs as:

Host-based IDS: gathers audit data from host audit trails aiming at detecting attacks against a single host

Distributed IDS: gathers audit data from multiple hosts and possibly the network connecting the hosts to detect attacks involving multiple hosts

Network-based IDS: uses network traffic as the audit data source, relieving the burden on hosts providing normal computing services

1.2.1.2 Insider Threat Detection

On the contrary, insider threat is defined by Liu, Martin, Hetherington and Matzner (2005) as "trusted users with legitimate access abusing system privileges" or as "intentionally

disruptive, unethical or illegal behaviour enacted by individuals possessing substantial internal access to organization's information assets (current/former employees, contractors, other trusted parties) by Mills, Grimaila, Peterson and Butts (2011). Insider attacks are indistinguishable or difficult to distinguish from normal actions as inside attackers have authorization to access and use the system and these actions are less likely to require changes to normal operation of applications and processes (Liu, et al., 2005). Database administration, word processing, web browsing, command-prompt interaction etc. are considered as normal activities, while exploitation, extraction, manipulation, reconnaissance, access and entrenchment are categorized as malicious insider activities. Table 1.1 categorizes these exploits into different types.

Mills, et al. (2011) further state that insider attacks are difficult to detect until after damage has been done and that attempts to solve these may exacerbate problems or introduce new problems. Yet, since most insider attacks are planned, there is a window of opportunity during which people can intervene before attack has occurred and prevent attack or limit damage (Mills, et al., 2011).

Table 1.1 – Exploits Identified from Insider Taxonomy and Captured as Malicious Behaviour (Source: Liu, et al., 2005)

Exploit Name	**Exploit Type**	**Description**
Privilege-escalation	Access/exploitation	Exploit local applications to gain root access
Removable media	Extraction	Copy or "Save As…" protected data to a zip or thumb drive
Export via e-mail	Extraction	Send protected data via e-mail
Change file extension	Manipulation	Change file extension to confuse sensors
Encipher / decipher	Manipulation	Encrypt or decrypt protected documents
Unusual search	Reconnaissance	User looks for system files or protected documents
Malware	Entrenchment	User attempts to download and install malware

1.2.2 Proactive & Sustainable Security

Even though most technical security measures may be somewhat sufficient to keep the outside attacks at bay, technical measures alone are clearly insufficient to ward off insider attacks. Vroom & von Solms state that: "Human behaviour is not performed according to a

set of written rules, but according to the personality of the individual… However, this behaviour can be categorized" (Vroom & von Solms, 2003). Mills, et al. (2011) propose a holistic approach blending people, process and technology by focusing on behaviours and activities appearing to be risky using a combination of risk management, functional analysis of insider behaviours and risk mitigation (evaluation and selection of control measures). Table 1.2 depicts the observable behaviours listed by Mills, et al. (2011).

It is stated that although cyber activities only provide limited insight into intent and character, they are easier to collect, process and correlate automatically. Additionally, background checks provide deterrence, but require further scrutiny. It is a duel-edged sword which should be used sparingly as too much information could damage privacy (Mills, et al., 2011).

Table 1.2 – Observables for Mitigating the Insider Threat (Source: Mills, et at., 2011)

Observables		
Polygraph results		
Failure to report	Finances, Travel, Contacts	
Violations	Physical security	
	Cyber security	
Physical access	Entry logs, ID badges	
Foreign travel		
Personal conduct	Finances, Wealth, Vices	
Materials transfer to handlers		
Social activity	Internal	
	External	
Counterintelligence		
Communications		
Cyber activity	Reconnaissance	Web browsing, Database (DB) searches, Network scans
	Entrenchment	Install sensors, Unauthorized software
	Exfiltration	Printouts, Downloads, Removable media
	Communication	Encrypted e-mails, Coded messages, Covert channels
	Manipulation	Permissions, Change data, Overwrite / Delete files
	Counter detection	Disk erasure, Overwrite / Deleting log files, Access human resource (HR) files
	Other actions	Improper information technology (IT) use, Pornography, Gambling

Sabett (2011) states that any security system should be designed by accepting that the "bad guys" are already inside the system, and instead of having a hardened shell and a soft core, the most sensitive parts of the system or network should be hardened.

Foley (2011) lists the following components as requirements for a proactive and sustainable security program:

Preventive: "knowing your customer" (credentialing the employees, clients and vendors) and restricting access (authorization of identity, time and place)

Detective: Auditing (user and subject reviews, random audits, risk-based audits and event-driven audits) and increasing security awareness and deterring inappropriate activity

Monitoring (automated forensic review of transaction logs for patterns of increased activity, activity outside normal business hours, access from unusual locations and indication of data mining)

Referrals (validate allegation and determine if the use was fraudulent or legitimate)

Corrective: Levels (additional monitoring or auditing, update credentials, access restriction or access removal) determined by assessing the extent of direct contribution by client to the compromise, the risk associated with the compromise and the risk that same incident could be repeated

Feedback: dynamic feedback (adjusting to changes in technology, legislation and threats), reactive and planned feedback, and creating and implementing solutions

1.2.3 Risk Perception Awareness

Gonzalez and Sawicka (2002) states that accidents will not normally happen if security measures stay above a certain threshold and the risk is kept below the "accident zone". In the typical life cycle of risk perception, perceived risk gradually declines when accidents do not occur as a consequence of improved security. Then the compliance with security measures also decline until system becomes vulnerable again. After a serious accident, risk perception soars, increasing compliance and starting a new cycle. This cycle (of perceived risk being out of phase with actual / current risk due to a perception delay, and accidents happening with increasing probability when current risk enters the accident zone) reoccurs a few times until a

fundamental lesson is learned (Gonzalez and Sawicka, 2002). Thus, they recommend risk perception renewals in order to sustain an appropriate level of risk perception through properly scheduled interventions such as security training and awareness programmes.

The ISO/IEC 27001 (2005) emphasizes the importance of training, awareness and competence by stating "The organization shall ensure that all personnel who are assigned responsibilities defined in the information security management system (ISMS) are competent to perform the required tasks by determining the necessary competencies for personnel performing work affecting the ISMS, providing training or taking other actions to satisfy these needs, evaluating the effectiveness of the actions taken and maintaining records of education, training, skills, experience and qualifications… The organization will also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives".

Peltier (2002) states that the level of awareness should be considered when developing security awareness programmes: Employees may be divided based on their current level of awareness of the information security objectives. One method of determining levels of awareness is to conduct a "walkabout" after normal working hours to look for key indicators such as whether the offices, desks and cabinets are locked, workstations, information and recording media are secured, etc. Personnel may also be categorized according to job category, job function, their knowledge about information processing and technology, system or application used, as well as level of awareness. It further discusses the methods used to convey the awareness message. "Showing how to do it is the best method of training most employees. They like the hands-on approach and want someone to answer questions. The best method for awareness is to watch a video on the subject. The message should stimulate the senses of the audience. An informed outsider presenting the message is more successful than a known messenger doing so. Employees tend to question the credibility of fellow workers. Absentees should be noted." It is further stated that awareness programmes must be scheduled around the work patterns of the audience and that the mornings on Tuesdays, Wednesdays or Thursdays would be the best (Peltier, 2002).

The solution proposed through this research incorporates these suggestions by blending social and technological methods and techniques to provide a managerial solution to address the problem of improper sharing of information by insiders with outsiders or unauthorized insiders, by monitoring the levels of observance of secure practices by the employees of an organization in order to create employee behavioural profiles by categorizing employees' security behaviour, and thus identifying employees whose actions could potentially lead to ISM problems and therefore require special education and training in ISM.

1.3 Related Work

Even though this research suggests the incorporation of profiling of employees' information security behaviour, criminal investigations is the prevailing area in the field of security where profiling is currently used. Thus, an understanding about criminal profiling will provide insight into profiling techniques which may be adaptable to information security.

1.3.1 Criminal Profiling

Criminal profiling is defined by Young and Varano (2006) as an investigative approach based on the premise that the crime scene provides details about the offense and the offender. It is used in investigations of homicide, sexual assault, arson, etc. Thompson (2011) defines criminal profiling as "the careful evaluation of physical evidence (collected and analyzed by a team of specialists from different areas) for systematically reconstructing the crime scene and developing a strategy to assist in capturing the offender and aiding trial, focusing on weeding out suspects, developing investigative strategy, linking crimes and suspects, and assessing risk". Based on the premise that "every criminal works to a certain set of values", criminal profiling is used to classify behavioural patterns and predict the next move assuming that offenders engaged in crime sprees devolve from lucid state of mind into a pathological state of frenzied criminality (Claridge, 2012). Examples of practical investigations which used criminal profiling include "Jack the Ripper", "New York Mad Bomber" and predicting Adolf Hitler's possible reactions during World War II (Young & Varano, 2006).

Criminal profiling entails examining evidence from crime scenes and victim and witness reports to develop an offender description containing (Winerman, 2004):

- Psychological variables: personality traits, psychopathologies and behaviour patterns
- Demographic variables: age, race, gender, emotional age, marital status, socioeconomic level, occupation, level of education, arrest and offense history, geographic location or residence relative to crime scene etc.

Criminal profiling uses geographic and psychological typologies to create a profile that isolates offender characteristics. Summarized below is the discussion of these typologies by Young and Varano (2006):

Geographically-based techniques: focus on the location of the crime scene to locate offender's home base by mapping offense locations. The "marauder" is an offender who branches out from a centralized home base to commit an offense, then returns to base. The "commuter" travels from a home base outside the offense area, while the "drifter" travels without a permanent base. The marauder and commuter models are familiar with the offense area. The commuter has access to transportation methods. Lack of financial backing geographically limits the criminal. *Investigative psychology* builds on geographic approach by analyzing additional crime scene variables (Young & Varano, 2006).

Psychologically-based techniques: compile psychological background using crime scene details and observable behaviours of offender's traits. Behaviour is interpreted from the presence or absence of forensic elements such as use of weapons and restraints, status of clothing, physical state of body, location of body disposal, means of approaching victim, etc. The "organized non-social offender" commits a planned crime and displays forensic awareness. This is usually a socially skilled, highly intelligent person maintaining a skilled occupation. The "disorganized asocial offender" leaves behind a disorganized scene and is usually a lone, isolated person with low impulse control and low financial credibility. Apart from the organized / disorganized dichotomy, psychological typologies are further classified into subcategories based on motivational factors (visionary, mission style, hedonistic or power-control type) and offense behaviours (power reassurance, power assertive, anger retaliatory or anger-excitation).

Criminal investigative analysis employs psychological typologies along with complete victimology (study of victims in many crimes perpetrated by the same criminal), police

reports, witness statements, autopsy reports, forensic reports, crime scene photographs to classify homicide type and construct profile, determine presence or absence of elements, amount of planning, degree of control, changes in emotional state during crime, risk level etc. *Behavioural evidence analysis* is a deductive approach where crime is studied individually as opposed to in comparison with previous cases, and a timeline is constructed and offender's behavioural choices, modus operandi and signature behaviours are evaluated. The resulting profile also includes evidence of criminal skill, relationship to victim, knowledge of crime scene's dynamics, familiarity with materials, and logical reasoning or justification for conclusions (Young & Varano, 2006).

Turvey (2000) states that inductive criminal profiling entails broad generalization and statistical reasoning and is thus subjective. On the other hand, deductive criminal profiling based on behavioural evidence analysis is preferred since it is a dynamic process which could be used to capture successful criminals whose methods either become more refined or deteriorated over time (Turvey, 2000).

Winerman (2004) states that the organized / disorganized dichotomy developed in 1974 by the behavioural science unit of the Federal Bureau of Investigation is challenged by psychologists who state that almost all serial murderers show some level of organization and that these core variables are frequently seen. These psychologists further state that the differences are seen in disorganized behaviours such as sexual control, mutilation and plunder, which divide criminals into categories. They suggest crime action profiling for developing models based on large studies (Winerman, 2004).

1.4 Research Objectives

This research addresses the problem of improper sharing of information by insiders with outsiders or unauthorized insiders and proposes a managerial solution, which employs a mix of technological and social methods and techniques to achieve internal control of information and communication within an organization. This solution entails security behavioural profiling, by monitoring cyber and non-cyber activities of users to detect the levels of observance of security best practices by the employees of the organization, detecting patterns among these behaviours, and using this information together with background information

and job details to create security behavioural profiles of users, to provide suggestions to information security officers and security managers to help identify users who might potentially pose threats to the organization's information security. Since insider attacks are difficult to detect using conventional intrusion detection techniques such as anomaly or misuse detection, a profiling system to predict potential behavioural patterns takes a step towards enabling insider threat detection. Further, the proposed solution will determine the level of security education or guidance to be given to each employee and schedule security education and training programmes will. In addition, periodic risk perception renewals will be scheduled in order to maintain the level of risk perception within an appropriate limit.

The next chapter discusses research methodology and explains how it is incorporated in this research. Chapter 3 provides the detailed explanation of the proposed concept and chapter 4 explains the design, implementation, and testing of the system to prove the feasibility of the concept proposed through this research, and discusses the engineering challenges faced, while the evaluation of system usability is discussed in chapter 5. Finally, chapter 6 summarizes this research, and states the conclusions of this research and future work which may be carried out.

Chapter 2

Research Methodology

Chapter 2

Research Methodology

2.1 Introduction

This research addresses the human-related information security problem of improper information sharing and presents a workable solution to predict the information security behaviour of employees of an organization by categorizing their behavioural patterns and profiling their security behaviour. In order to do so, it is important to gain an in-depth understanding of human behavioural heuristics and personalities. Thus, the subsequent subsections discuss these aspects of human behaviour. The rest of this chapter studies the methodology adapted in this research to profile human behaviour.

2.1.1 Human Behavioural Heuristics

According to the American Association for the Advancement of Science (AAAS), humans are a species living in the company of other humans. The AAAS (1990) states that human behaviour is affected by humans. Humans are organized into social groupings in which they live. Deliberate changes in social behaviour and organization over time are combined with socialization, resulting in different complex and dynamic patterns of human society across space, time and cultures. Social scientists study human behaviour from cultural, political, economic and psychological perspectives, looking for consistent patterns of individual and social behaviour and both scientific and genetic inheritance and experience. The characteristics of the social and cultural setting, such as family, community, social class, language and religion a person is born into affect how he thinks and behaves. In addition to the means of instruction, example, and rewards and punishment, one's thoughts and behaviour are also influenced by informal interactions with friends, peers, relatives and media. Technology has always played a major role in human behaviour, leading to rapid spread of fashions and ideas through international travel and mass media, and implicitly promoting

values, aspirations, priorities and attitudes. Acceptable human behaviour varies from culture to culture and time to time. Unusual behaviour could be considered amusing, distasteful or punishable. For instance, aggressively competitive behaviour is considered rude in highly cooperative cultures, while lack of competition is regarded lazy in others.

West (2008) explains how risk and uncertainty are difficult concepts for people to evaluate. "Fundamentally, the user problem in security systems is about how people think of risks that guide their behaviour… Basic principles of human behaviour that govern how users think about security in everyday situations show why they undermine security accidents." Predictable and exploitable characteristics in the human decision-making process include the belief that they are at less risk, risk homeostasis (maintaining an acceptable degree of risk and increasing risky behaviour to suit increased security measures), cognitive miserliness (having a limited capacity for information processing and multitasking) leading to quick, uninformed decisions based on learned rules and heuristics, feeling less motivated by abstract concepts like security, incorrect evaluations of trade-off between security and cost, and perceiving loss disproportionately to gains. West (2008) concludes that for many people, security becomes a priority only when they have problems with it. This study clarifies why people from different cultures react in different ways concerning information security.

Bruce Schneier (2008) conducts a closer examination of these heuristics. He states that "security is both a feeling and a reality". While the reality is mathematical, based on the probability of different risks and effectiveness of different countermeasures, the feeling is based on one's psychological reactions to risks and countermeasures. One can be secure without feeling secure (paranoia), and vice versa. Schneier (2008) attempts to find why this feeling of security diverges from the reality by researching about behavioural economics (emotional, social and cognitive human biases), psychology of decision-making and bounded rationality, psychology of risk and risk perception, and neuroscience (how human brains have developed complex mechanisms to deal with threats). Any gain in security involves trade-offs in terms of money, time, convenience, capabilities or liberties. Humans make trade-offs intuitively, exaggerating some risks or costs, while downplaying others. Aspects of trade-off such as the severity of the risk, probability of the risk, magnitude of the costs, effectiveness of countermeasures at mitigating the risk, and comparison of disparate risks and costs, can go

wrong. The more the perception diverges from reality, the more the perceived trade-off diverges from the actual trade-off. Reasons for incorrect perception of risks are listed in Table 2.1.

Table 2.1 – Conventional Wisdom about People and Risk Perception (Source: Schneier, 2008)

Exaggerated risks	**Downplayed risks**
Spectacular	Pedestrian
Rare	Common
Personified	Anonymous
Beyond their control or externally imposed	More under their control or taken willingly
Talked about	Not discussed
Intentional or man-made	Natural
Immediate	Long-term or diffuse
Sudden	Evolving slowly over time
Affecting them personally	Affecting others
New and unfamiliar	Familiar
Uncertain	Well understood
Directed against their children	Directed towards themselves
Morally offensive	Morally desirable
Entirely without redeeming features	Associated with some ancillary benefit
Not like their current situation	Like their current situation

Human risk perception fails because new situations have occurred at a faster rate than human evolution (Schneier, 2008). The “amygdala”, a primitive part of the brain, processes base emotions from sensory inputs like anger, avoidance, defensiveness, and fear, triggering the fight-or-flight response. Yet, some situations are better handled by sophisticated analysis of situation and options using the “neocortex”, a recently developed part of the brain in mammals. Having two systems operating in parallel makes people feel both rational and flighty at the same time. Unfortunately, this newer innovation of the brain is still in its early stages of development, resulting in many miscalculations. Instead of evaluating security trade-offs mathematically, humans use shortcuts, rules of thumb, stereotypes, and biases, known as heuristics, to generate answers quickly, with limited cognitive capabilities. Schneier (2008) explains these heuristics and theories through many scientifically conducted

experiments. These behavioural heuristics, which may affect the way people react to ISM-related problems, are summarized in the remainder of this subsection.

2.1.1.1 Risk Heuristics

- Prospect Theory – Kahneman and Tversky (1979) state that humans accept small sure gains rather than risking / chancing a larger gain, and risk / chance larger losses rather than accepting smaller sure losses
- Endowment Effect – humans value something more when represented as something that can be lost, as opposed to a potential gain
- Optimism Bias and Control Bias – humans believe that good outcomes are more probable than bad outcomes, and are more likely to accept risks they feel they have some control over
- Affect Heuristic – an overall good feeling toward a situation leads to a lower risk perception, while an overall bad feeling leads to a higher risk perception

2.1.1.2 Probability Heuristics

- Small numbers matter more than large numbers (a half, a quarter, one eighth, or almost nothing)
- Availability Heuristic and Hindsight Bias – humans consider something that is more available to be more probable (common events, vivid and salient arguments) and consider events that have actually occurred previously to be more probable
- Representativeness and Law of Small Numbers – humans assume that the probability that an example belongs to a particular class is based on how closely that example represents the class, and that long-term probabilities also hold true in the short run

2.1.1.3 Cost Heuristics

- Mental Accounting – humans have different mental budgets and may be willing to accept considerable risks in one mental account, but would not consider them if charged against a different account
- Time Discounting – humans tend to discount future costs and benefits
- Magnitude Effect – smaller amounts are discounted more than larger ones
- Framing Effect – framing something as an acceleration or a delay from a base reference point

2.1.1.4 Decision Heuristics

- Context Effect – humans tend to choose options that dominate other options, or compromise options that lie between other options (avoiding extremes)
- Choice Bracketing – humans choose a more diverse set of items when the decision is bracketed more broadly than when bracketed more narrowly
- Anchoring Effect – human decisions are affected by random information cognitively nearby (mentally adjusting facts to suit facts anchored in their minds)
- Confirmation Bias – humans are more likely to notice evidence supporting a previously held position rather than evidence that discredits it

2.1.2 Personality Types

Lacey (2009) states that the Myres-Briggs Type Indicator (MBTI) tool could be used to categorize human psychological types, which may explain the information security behaviour of different employees of an organization. This subsection discusses how different behavioural traits linked to different human personality types may be categorized.

Carl Jung's Theory of Psychological Types, introduced in the 1920s, states that much seemingly random variation in behaviour is actually quite orderly and consistent, being due to

basic differences in the way individuals prefer to use their perception and judgement. According to the Myers & Briggs Foundation, MBTI, developed by Isabel Briggs Myers and Katharine Briggs in the 1940s, makes this theory understandable and useful. MBTI is based on Jung's ideas about perception and judgement and the attitudes in which these are used in different types of people, to identify basic preferences of each of the four dichotomies specified or implicit in Jung's theory and to identify and describe the sixteen distinctive personality types resulting from the interactions among the preferences. 'Perception' is defined as "all the ways of becoming aware of things, people, happenings or ideas", while 'Judgement' is defined as "all the ways of coming to conclusions about what has been perceived." It is further stated that if people differ systematically in what they perceive and in how they reach conclusions, then it is only reasonable for them to differ correspondingly in their interests, reactions, values, motivations, and skills (The Myers & Briggs Foundation). The four dichotomies explained by the Myers & Briggs Foundation are summarized below:

- Favourite world: Extraversion or Introversion (E-I) are mutually complementary attitudes. The tension generated by the differences is needed for maintenance of life. "Extraverts" are oriented primarily toward the outer world and tend to focus their perception and judgement on people and objects, while "introverts" are primarily oriented toward the inner world and tend to focus their perception and judgement upon concepts and ideas.
- Information: Sensing or Intuition (S-N) are opposite ways of perceiving information, either focusing on basic information or interpreting and adding meaning. "Sensing" relies primarily upon the process of sensing, which reports observable facts or happenings through one or more of the five senses, while "intuition" relies upon the less obvious process of intuition, which reports meanings, relationships and / or possibilities that have been worked out beyond the reach of the conscious mind.
- Decisions: Thinking or Feeling (T-F) are contrasting ways of judgement, either looking at logic and consistency or looking at people and special circumstances. "Thinking" relies primarily on thinking to decide impersonally on the basis of logical consequences, while "feeling" relies on feelings to decide primarily on the basis of personal or social value.

- Structure: Judging or Perceiving (J-P) are processes used in dealing with the outer world (i.e.: the extraverted part of life). “Judging” uses a judgement process (either “thinking” or “feeling”) for dealing with the outer world and thus get things decided, while “perceiving” uses a perceptive process (either “sensing” or “intuition”) for dealing with the outer world and stay open to new information and options.

One pole of each of the four preferences is preferred (dominant) over the other pole (auxiliary) and these preferences on each index are independent of preferences for the other three indices. Thus, the four indices yield sixteen possible combinations called “types”, with each type having its own pattern of dominant and auxiliary processes and the attitudes (E or I) in which these are habitually used. The characteristics of each type follow from the dynamic interplay of these processes and attitudes (The Myers & Briggs Foundation). Table 2.2 lists these sixteen personality types.

Table 2.2 – The Sixteen Personality Types (Source: The Myers & Briggs Foundation)

ISTJ	ISFJ	INFJ	INTJ
ISTP	ISFP	INFP	INTP
ESTP	ESFP	ENFP	ENTP
ESTJ	ESFJ	ENFJ	ENTJ

The Myers & Briggs Foundation classifies these 16 personality types as having the characteristics listed in table 2.3. Lacey (2009) states that the ideal profile for a criminal mastermind INTJ, a highly organized planner and capable leader. These types are rare in the general population, but are found in a few IT directors (Lacey, 2009). He further states that a lone fraudster, being a shy, analytic loner in good company would likely belong to the INTP type. Carl Jung, himself, was of INTP type (Lacey, 2009).

Table 2.3 – Characteristics of the Sixteen Personality Types (Source: The Myers & Briggs Foundation)

Type	Characteristics of Personality
ISTJ	Quiet, serious, earn success by thoroughness and dependability. Practical, matter-of-fact, realistic, and responsible. Decide logically what should be done and work toward it steadily, regardless of distractions. Take pleasure in making everything orderly and organized – their work, their home, their life. Value traditions and loyalty.
ISFJ	Quiet, friendly, responsible, and conscientious. Committed and steady in meeting their obligations. Thorough, painstaking, and accurate. Loyal, considerate, notice and remember specifics about people who are important to them, concerned with how others feel. Strive to create an orderly and harmonious environment at work and at home.
INFJ	Seek meaning and connection in ideas, relationships, and material possessions. Want to understand what motivates people and are insightful about others. Conscientious and committed to their firm values. Develop a clear vision about how best to serve the common good. Organized and decisive in implementing their vision.
INTJ	Have original minds and great drive for implementing their ideas and achieving their goals. Quickly see patterns in external events and develop long-range explanatory perspectives. When committed, organize a job and carry it through. Skeptical and independent, have high standards of competence and performance – for themselves and for others.
ISTP	Tolerant and flexible, quiet observers until a problem appears, then act quickly to find workable solutions. Analyze what makes things work and readily get through large amounts of data to isolate the core of practical problems. Interested in cause and effect, organize facts using logical principles, value efficiency.
ISFP	Quiet, friendly, sensitive, and kind. Enjoy the present moment, what's going on around them. Like to have their own space and to work within their own time frame. Loyal and committed to their values and to people who are important to them. Dislike disagreements and conflicts, do not force their opinions or values on others.
INFP	Idealistic, loyal to their values and to people who are important to them. Want an external life that is congruent with their values. Curious, quick to see possibilities, can be catalysts for implementing ideas. Seek to understand people and to help them fulfil their potential. Adaptable, flexible, and accepting unless a value is threatened.
INTP	Seek to develop logical explanations for everything that interests them. Theoretical and abstract, interested more in ideas than in social interaction. Quiet, contained, flexible, and adaptable. Have unusual ability to focus in depth to solve problems in their area of interest. Skeptical, sometimes critical, always analytical.
ESTP	Flexible and tolerant, they take a pragmatic approach focused on immediate results. Theories and conceptual explanations bore them – they want to act energetically to solve the problem. Focus on the here-and-now, spontaneous, enjoy each moment that they can be active with others. Enjoy material comforts and style. Learn best through doing.
ESFP	Outgoing, friendly, and accepting. Exuberant lovers of life, people, and material comforts. Enjoy working with others to make things happen. Bring common sense and a realistic approach to their work, and make work fun. Flexible and spontaneous, adapt readily to new people and environments. Learn best by trying a new skill with other people.
ENFP	Warmly enthusiastic and imaginative. See life as full of possibilities. Make connections between events and information very quickly, and confidently proceed based on the patterns they see. Want a lot of affirmation from others, and readily give appreciation and support. Spontaneous and flexible,

	often rely on their ability to improvise and their verbal fluency.
ENTP	Quick, ingenious, stimulating, alert, and outspoken. Resourceful in solving new and challenging problems. Adept at generating conceptual possibilities and then analyzing them strategically. Good at reading other people. Bored by routine, will seldom do the same thing the same way, apt to turn to one new interest after another.
ESTJ	Practical, realistic, matter-of-fact. Decisive, quickly move to implement decisions. Organize projects and people to get things done, focus on getting results in the most efficient way possible. Take care of routine details. Have a clear set of logical standards, systematically follow them and want others to also. Forceful in implementing their plans.
ESFJ	Warm-hearted, conscientious, and cooperative. Want harmony in their environment, work with determination to establish it. Like to work with others to complete tasks accurately and on time. Loyal, follow through even in small matters. Notice what others need in their day-by-day lives and try to provide it. Want to be appreciated for who they are and for what they contribute.
ENFJ	Warm, empathetic, responsive, and responsible. Highly attuned to the emotions, needs, and motivations of others. Find potential in everyone, want to help others fulfil their potential. May act as catalysts for individual and group growth. Loyal, responsive to praise and criticism. Sociable, facilitate others in a group, and provide inspiring leadership.
ENTJ	Frank, decisive, assume leadership readily. Quickly see illogical and inefficient procedures and policies, develop and implement comprehensive systems to solve organizational problems. Enjoy long-term planning and goal setting. Usually well informed, well read, enjoy expanding their knowledge and passing it on to others. Forceful in presenting their ideas.

Lacey (2009) emphasizes that MBTI can indicate who is likely to commit a fraud, but cannot explicitly state who will commit a fraud. In this research MBTI is used for validating the behaviours profiled by the developed system.

2.2 Adapted Methodology

Of the different candidate theoretical models, frameworks, and approaches, such as rule-based inference systems, Hidden Markov Model, machine learning, etc, that could be adapted by this system for profiling information security behaviour, the most appropriate approach for developing this knowledge system was rule-based inference systems, because of their ability to simulate the process of human decision-making. The following subsection explains this methodology in detail.

2.2.1 Rule-Based Inference System

As opposed to traditional programming systems, which are sequential and follow a fixed execution path, in rule-based inference systems, the next rule to be executed is determined by

the knowledge within (Enterra Solutions, 2014). Allowing the knowledge to be expressed in a pure form and invoking the applicable rule is an ideal way of programming a knowledge system simulating human thought (Enterra Solution, 2014). In a rule-based inference system, the user provides information about the problem to be solved and the system attempts to provide insights derived or inferred from examining the knowledgebase (Griffin & Lewis, 1989). According to Platt (2000), the expertise used by a person to perform an expert task can often be represented as rules. Rule-based inference systems allow a collection of discrete rule to represent judgemental knowledge regarding a specific problem, where each rule states that if certain premises are known, then certain conclusions can be inferred (Duda, Hart, Nilsson & Sutherland, 1977).

These rules (also known as production rules) are of the following form:

if <conditions> then <actions>

where, the actions are executed if the conditions are satisfied (Griffin & Lewis, 1989). The set of statements following the word “if” represent observable patterns, whereas, the statements following the word “then” represents conclusions that may be drawn or actions that may be taken based on those conclusions (Platt, 2000). Thus, a rule-based inference system identifies a pattern and draws conclusions regarding its meaning and / or advises the actions needed to be taken regarding it, thus, making a rule-based inference system, the best approach for this research.

Similar to a human following a chain of ideas to reach a conclusion, a rule-based reasoning system goes through a series of cycles, producing new information through the execution of each rule, and thereby, taking the reasoning process further in each cycle (Platt, 2000). The radical difference between a conventional software program containing an “if… then…” structure and a production system, is that a production system can choose a rule appropriate to the current circumstances from the knowledgebase to execute. The “recognize-act cycle” of an inference engine checks for matches between the data in the working memory and the condition of a rule to fire that particular rule (Platt, 2000). Since knowledge can easily be expressed as a set of production rules, they provide notational convenience, and the rule base could be expanded by simply adding more rules at the end of the rule base (Platt, 2000).

There are two methods of inference used by rule-based inference systems (Griffin & Lewis, 1989):

- Forward chaining: a top-down exploration method, which considers facts as they become available and attempts to draw conclusions from and execute actions of the rules that have all their conditions satisfied
- Backward chaining: a bottom-up verification procedure, which begins with the goals / actions and queries the user about information which may satisfy the conditions contained in the appropriate rules

A forward chaining process will be used in simulating a game of chess where it begins with the current facts – the position of the pieces on the chess board – and applies rules of piece-movement in a goal-directed way to attempt to checkmate the opponent (Enterra Solutions, 2014). An example for backward chaining is when the user begins with an objective and reasons backward to figure out how to satisfy that objective, such as figuring out whether to buy or bake a cake if the user wants to eat cake and figuring out a store, transportation to get to the store, the cost, etc. in order to conclude whether to buy or bake the cake (Enterra Solutions, 2014).

The implementation of the system proposed through this research uses a forward chaining process to profile user information security behaviour based on the observed or monitored behavioural characteristics and schedules security education and training accordingly. As a conflict resolution strategy to decide which rules are fired first, this system uses the method where the rules listed first are executed first if all of their conditions are satisfied.

Chapter 3

Proposed Concept

Chapter 3

Proposed Concept

3.1 Introduction

The system proposed through this research to achieve internal control of information and communication within an organization is explained in detail in this section.

This system addresses the threat of improper sharing of information, both intentional and unintentional, by authorized insiders, with outsiders or other unauthorized insiders. Even though most systems acknowledge the importance of focusing on the human factor in information security, most currently available efforts focus on technological solutions only. Yet, people easily bypass technological controls and restrictions. Thus, this research proposes a managerial solution employing a mix of social and technological methods and techniques by monitoring the level of observance of secure practices by the employees of an organization, creating user behavioural profiles based on this data along with background information and job details, identifying users whose behaviour might lead to security problems and infractions in the future and providing them with education and training in ISM.

3.2 Overall System

Lacey (2009) has pointed out that curtailing or limiting the personal browsing ability of employees is detrimental to their productivity. Yet, depending on the project(s) the employee is working on and the criticality of the business information the employee has to access, it is sometimes mandatory to restrict web browsing and access to the Internet in order to protect the security of the business information used for the project. In some instances, the clients themselves request such restrictions. This system addresses this problem by providing two separate modes: the “strict” mode and the “relaxed” mode.

During the “strict” mode, which is the default mode:

- Only pre-specified programs and services are allowed (all others are denied)
- All activities are monitored
- All activities are logged
- All retrievals, printing and copying of information are logged and copies of files are tagged
- Only work-related activities are allowed
- No personal browsing, personal e-mails or instant messaging etc. are allowed
- All information exchanges (e-mail contents, e-mail attachments, file sharing etc.) are recorded

The “relaxed” mode must specifically be activated and these activation and deactivation times are logged and used for profiling and performance evaluations. During the “relaxed” mode:

- Personal browsing, personal e-mails, instant messaging etc. are allowed
- Personal activities are not monitored (to protect user privacy)
- No access to work-related information (databases etc.) are allowed
- E-mail attachments and file sharing are recorded
- Contents of excessively long e-mails are recorded

The use of two separate modes also helps to address the privacy implications produced by monitoring user activity, by clearly distinguishing between the times when monitoring will or will not take place. Having only two separate modes allows for higher productivity and minimizes privacy concerns while maintaining simplicity by avoiding complications produced by a multi-modal system containing a multitude of different modes.

The subsequent subsections explain the system functions and the user classes of the proposed system and their characteristics in detail.

3.2.1 System Functions

The system will constantly monitor for extraordinary behaviour:

- Excessive access to information, services or systems
- Untimely access to information, services or systems
- Access from remote terminals
- Trying to access data of a higher classification level than the user's security clearance level
- Trying to access data for which the user has no Need-to-Know according to the user's job description

Once such extraordinary behaviour is detected, the system will automatically switch to strict mode. Switching back to relaxed mode once an automatic switch has occurred requires permission from the Information Security Officer (ISO) or a security manager. The system automatically monitors all user access to digitized information. It is important to note that even though the information concerned is not digitized, the proposed system can provide useful information, to a certain extent, to detect malicious access because the system has a function which allows employees' managers or security personnel of the organization to observe employees' access to not only digitized data, but also to non-digitized / non-machine-readable data. The behavioural traits observed through the monitoring of cyber and non-cyber access to information, and predicted through the compiled security behavioural profiles, may also give an indication of the likelihood that an employee would share human-readable information or mental information with others.

The system will also constantly monitor cyber and non-cyber activities of its employees to determine their levels of observance of best practices. In order to cover as many categories of security behaviour as possible, the following aspects are looked into:

<u>Password Security Behaviour</u>:

- Password strength (difficulty of remembering password, difficulty of guessing password, obviousness, etc.)
- Frequency of changing password

- Reuse of former passwords
- Whether the password is saved
- Whether the password is often mistyped
- Whether the password is often forgotten
- Time taken to type password
- Time taken to get used to typing a new password
- Whether the same password is shared across different applications
- Whether passwords are shared with others

Data Backup Behaviour:

- Frequency of data backup (both company data and personal data, and both hard backup and soft backup)
- Whether the backup naming conventions are properly observed

Data Sanitization Behaviour:

- Whether unnecessary copies of data are destroyed (both hard copies and soft copies)
- Sanitization of external storage media
- Whether access to personal storage media is controlled (whether they are lent to or freely accessible by others, whether they are used from different terminals, etc.)
- Use of others' storage media (whether they are scanned before using, whether they are sanitized before returning, etc.)
- Whether temp files, cookies, history, saved passwords, etc. are deleted

Network Security Behaviour:

- Whether firewalls are enabled (whether they are relaxed to allow different applications access to the system, whether privilege is escalated to allow installation of software, whether escalated privileges are reset after installation of programs, etc.)
- Whether antivirus software is periodically updated
- Whether computers are periodically scanned
- Checking authenticity of websites, e-mail attachments, etc. before clicking on links or opening attachments

- Validating credentials of people before correspondence

Physical Security Behaviour:

- Visibility of monitor
- Awareness of surrounding (whether others such as maintenance crew, janitors, etc. are around)
- Locking computer when leaving the desk
- Locking cupboards, desks, office, vehicle, etc.
- Whether confidential or personal items are left behind unattended (documents, computers, storage media, password hints, etc.)
- Whether personal items are shared with others
- Whether unknown items are used without validation
- Forgetting, lending or borrowing keys

Cyber activities of users such as password renewal frequency, reuse of former passwords, password strength, data back-up frequency etc. will be regularly monitored automatically by the security system. Non-cyber activities such as whether the users leave confidential documents lying around, whether doors are locked, whether they talk openly about work-related things with co-workers etc. will be monitored personally by their managers or the security personnel of the organization. Cyber activity monitored by the system will be stored separately, in parallel with other non-cyber activities monitored by managers and security personnel. Managers and security personnel can perform a walk-through after office hours to gather information about non-cyber activities.

Non-cyber activity and background information will be personally inputted into the system by managers, security personnel and human resource (HR) managers:

- Personal views about the behaviour of employees will be inputted by the managers and security personnel. *This information will help in identifying personality traits of employees, whether they feel isolated from their peers, whether they feel pressurized under competition, whether they can be easily enticed or tricked into revealing information, etc.*
- Information from background checks before employment and periodically during

employment are inputted to the system by human resource managers. These include: contact details, financial status and stability, number of dependents, educational level, criminal record, etc. *This information will help in identifying users that might be enticed to reveal information for financial or career-wise incentives etc.*

- Employee's job description will be inputted or updated by his manager according to the project(s) the employee is currently working on. Responsibility entailing the job and the records of performance evaluations will be included. *This information would help in identifying users that try to access information above their security clearance level or for which they do not have a Need-to-Know, and users that might be enticed to reveal information for career-wise incentives etc.*

This information, together with other cyber-activity related information automatically gathered by the system is used for profiling and for finding the behavioural types each of the employees belong to. The resulting security behavioural profiles will include:

- The security consciousness of the employee
- The extent of understanding of the security policy by the employee
- The value given to ISM rules and procedures by the employee and the extent of adherence to policies
- How easily information is revealed to others
- How easily an employee can be enticed or tricked into revealing information to others
- Employee's ambitiousness and drive to move ahead in his or her career
- Employee's sociability, capability to work in a team and respect gained by peers
- The potential of an employee to intentionally or unintentionally reveal or improperly share confidential information with others
- Whether the employee has any motive or incentive (financial, career-wise, social, psychological or personal) to access unauthorized information or reveal information to others

Through the behavioural profiles created, the system then provides suggestions to the ISO / security managers to help them identify potentially problematic employees, and determines the level of education, training or guidance on security awareness required by them. Depending on the extent of problematic behaviour, awareness and training programmes could

range from pop-up notifications to workshops conducted by security professionals. The extent of the required awareness and training programme is calculated and determined by the system. If pop-up security awareness reminders or visual aids such as presentations are sufficient, the system automatically conducts these awareness programmes through the identified employee's computer. If more extensive training programmes or workshops are required, the system schedules such programmes and notifies the security managers, who then conduct such programmes with the help of outside security professionals. In addition to planned and scheduled awareness and training programmes for identified problematic users, the system also periodically schedules awareness and training programmes for all users at random intervals, in order to maintain a high level or security awareness by all employees. Based on the resulting behavioural profiles the security awareness, guidance, or training may be:

- Planned and scheduled awareness and training programmes for identified potentially problematic users
- Randomly scheduled awareness and training programmes for all users, periodically, as risk perception renewals to maintain the desired level of security awareness
- In the case of extensively problematic behaviour by an employee being detected by the system, it immediately alerts the ISO in real-time so that he or she may act immediately and take the necessary steps to prevent the security breach or minimize the damages incurred by the breach. The ISO may take steps such as immediately barring access to the system, services, network and organization's information by the identified employee, and informing the relevant authorities such as police and federal agents, depending on the severity of the breach and incurred damage.

The security managers and the ISO can request to view behavioural profiles and security education and training schedules in the following ways:

- Security managers and the ISO can request to view behavioural profiles of users in summarized, detailed or graphical form
- Training schedules for employees can also be viewed by security managers and the ISO
- The ISO can additionally also request separate views of automatically monitored (cyber-activity-related) data and personally inputted (non-cyber-activity-related) data and thus

use his or her personal judgement to avoid any personal bias the managers or security personnel might have towards any employee

Figure 3.1 depicts the top-level architectural design of the proposed system.

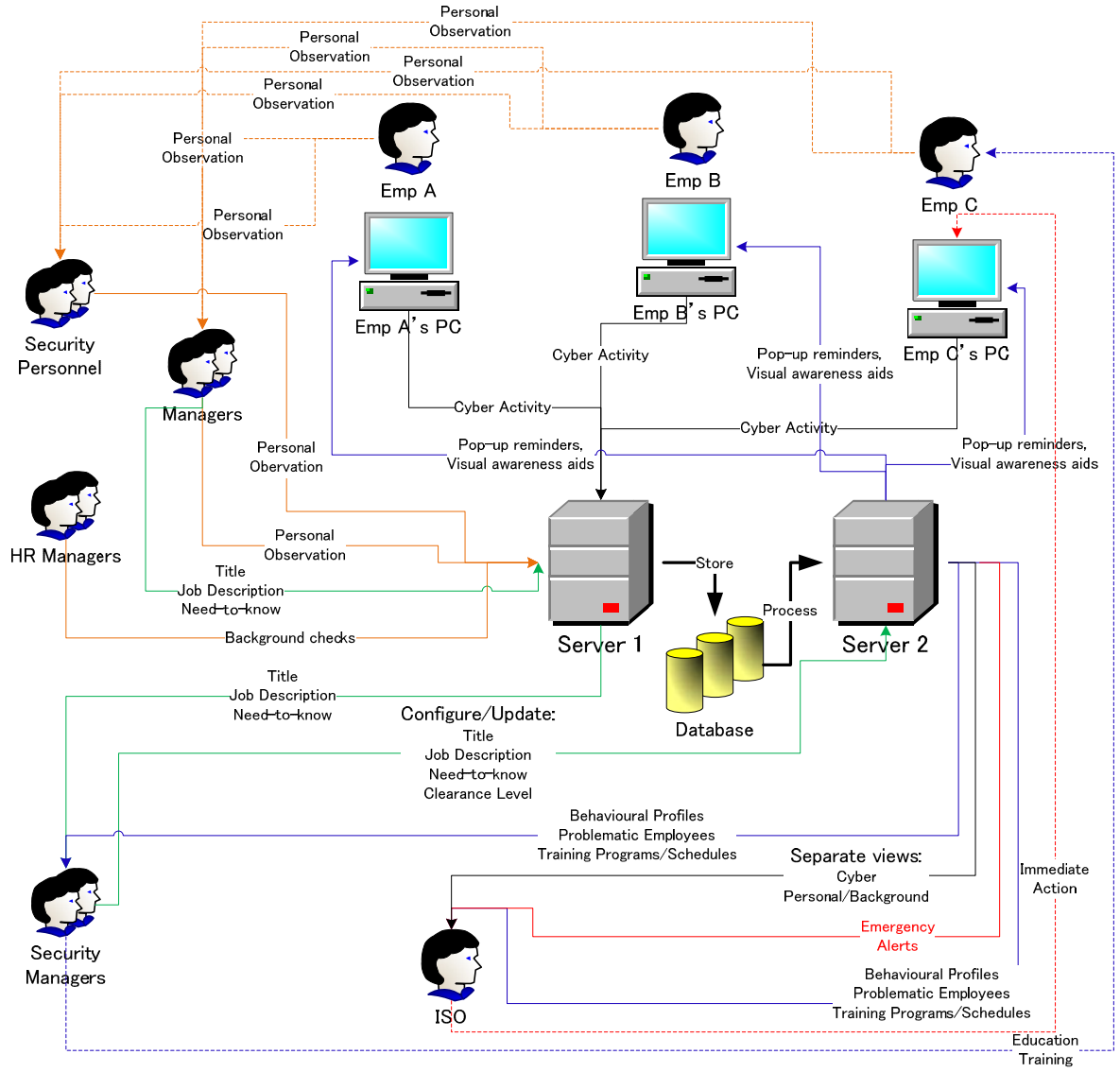

Figure 3.1 – Top-Level Architectural Design of the Proposed System

Given below are some possible example scenarios of detecting problematic employees using this proposed system:

- Employee A is a senior accountant in charge of handling employee salaries. She is financially well established with good academic and professional qualifications and is at

the peak of her career. Yet, if a colleague asks to use her computer for some personal purpose, she provides them with her authentication information in order to help them. *Employee A has no career-wise, personal, or financial motives for intentional violation of the company's information security. Yet, she can be easily tricked into revealing confidential information and thus, is an easy target of social engineering.* She needs a security training workshop to make her understand the risks of a security breach, along with periodic automatic reminders of secure information sharing practices.

- Employee B is a software analyst and is in serious financial crisis. He tries to access employee salary information for which he has no Need-to-Know. *Employee B may be trying to intentionally violate the confidentiality and integrity of the organization's salary information.* The ISO must closely monitor his activities and de-escalate his privileges and security clearance to restrict access.

3.2.2 User Classes & Characteristics

The different user classes in this system and their characteristics are as follows:

- Employees – Do not input any information into the system. Their cyber activities are monitored by the system and behavioural patterns are detected. Direct interaction with the system occurs only when the system provides automatic security awareness training to the employees in the form of either pop-up reminders or visual aids.
- Managers – Observe employees working under them and input their personal views about the employees' security consciousness and non-cyber behaviour in to the system. They also input or update the employees' job titles, job descriptions and Need-to-Know depending on the projects they are currently working on.
- Security Personnel – Observe employees and input their personal views about the employees' security consciousness and non-cyber behaviour in to the system.
- Human Resource Managers – Conduct background checks on employees during recruitment and periodically thereafter and input background information to the system.
- Security Managers – View summaries, details, graphs and charts on employees' security behavioural patterns and profiles. View security awareness education and training programmes scheduled by the system for each employee and conducts extensive training programmes or workshops with the help of outside security professionals.

- Information Security Officer - Views summaries, details, graphs and charts on employees' security behavioural patterns and profiles. Views separate views on employees' security behaviour categorized under cyber activities monitored directly by the system, personal views inputted by their managers or security personnel, and background information inputted by the HR managers. Views security awareness education and training programmes scheduled by the system for each employee. Views emergency alerts in case of a security breach and takes immediate action based on the severity of the breach. Configures the security rules of the profiling system to be aligned with the business objectives of the organization.

3.2.3 Client-Server Architecture

This system employs a client-server architecture where the system hosted on a server provides different services to the different user classes discussed in the preceding section. The subsequent subsections examine the system features provided to these different user classes and their use cases.

3.2.3.1 System Features

User Log In

A user enters user ID and password and clicks "Log In" button →

Log In Success:

Saves user ID, date, and time in the audit log. Depending on the user's designation, his or her user category is identified:

Employee: Taken to the Mode Selection page.

Manager: Taken to the Manager's Tasks page allowing the choice of the Input Personal View page or the Input / Update Job Details page.

Security Personnel: Taken to the Input Personal View page.

Human Resource Manager: Taken to the HR Manager's Tasks page allowing the choice of the Add New Employee page or the Input / Update Background Information page.

Security Manager: Taken to the Request Behavioural Profiles page.

Information Security Officer: Taken to the ISO's Tasks Page allowing the choice of the Request Behavioural Profiles page or the Configure Security Rules page.

Log In Fail:

Saves IP address, date, and time in the audit log. User is returned to the Log In page. If the third attempt at Log In fails, the IP address is blocked and the ISO and security managers are immediately notified.

Figure 3.2 depicts the log-in activity of the system.

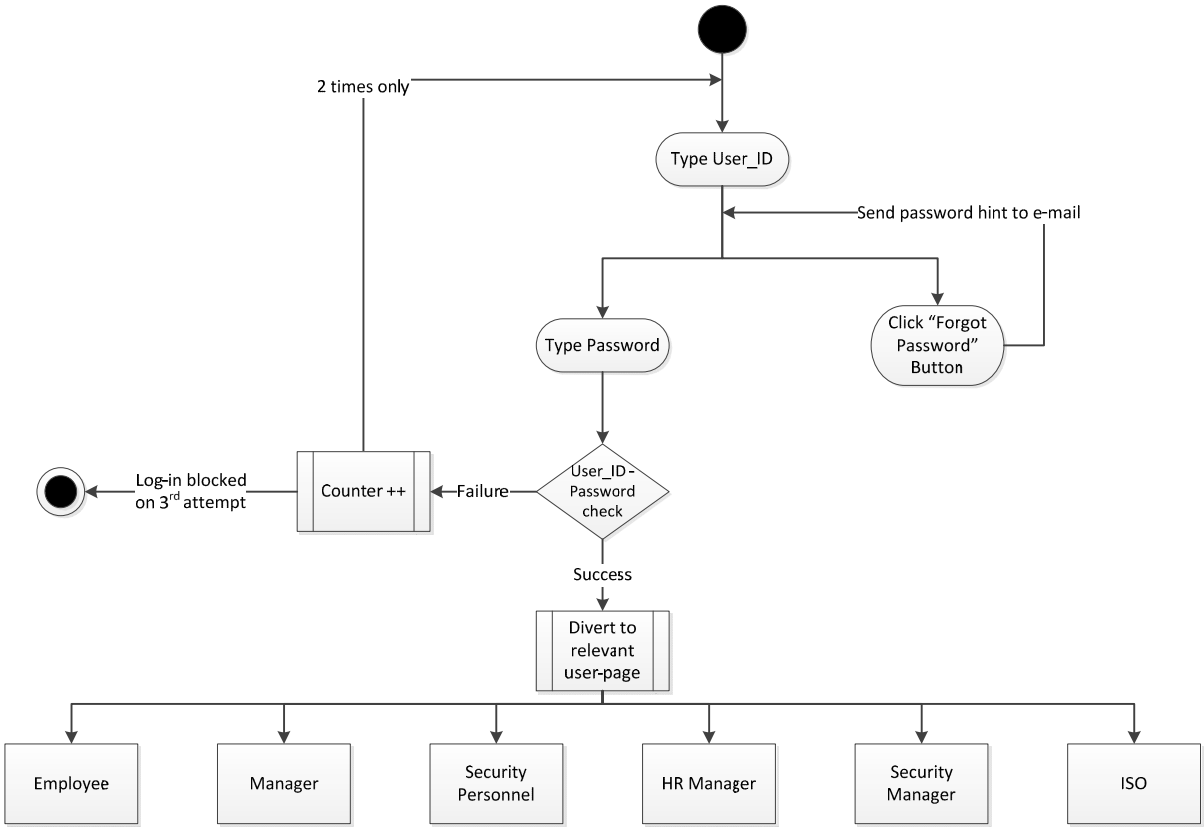

Figure 3.2 – Activity Diagram for Log-In

Mode Selection

The default mode is the Strict mode. If an employee selects the Relaxed mode and clicks the "OK" button →

> Saves employee ID, date and time in the audit log and the employee is taken to relaxed mode. The employee's personal browsing is enabled, while access to organization's information database is denied.

If user selects Strict mode and clicks "OK" button →

> Saves employee ID, date, and time in the audit log. The time spent on the Relaxed mode is calculated and stored in the system database. Personal browsing is disabled, while access to the organization's information is granted according to the employee's security clearance level and Need-to-Know.

Pop-up Security Awareness Reminders and Visual Aids

Security awareness reminders or visual aids such as presentations pop-up in the employee's computer monitor at randomly scheduled instances or when the user is identified by the system to be potentially problematic to the organization's security. The employee can return to work once the reminders or presentations followed by a question and answer (Q&A) session are successfully completed.

Input Personal Views

A manager or security personnel selects an employee working under him or her, or in the division he or she is working in, from the drop down box and clicks "Input Personal View" button →

> The manager or security personnel is taken to the page to input their personal views on the employee's behaviour. Once the manager or security personnel types in his or her personal view on the employee's non-cyber behaviour and clicks the "OK" button, the personal views are saved in the system database.

Input or Update Job Details

When an employee is promoted, selected for a new project or removed from his or her current project, his or her manager selects that employee from the drop down box and clicks "Input / Update Job Details" button →

> The manager is taken to the page to input or update employee's job title, job description and need-to-know. The manager modifies the current field(s) and clicks the "Update" button(s) and the updated values are saved in the system database.

Input or Update Employee Background Information

When a background check is conducted on an employee, a human resource manager selects the employee from a drop down box and clicks "Input / Update Background Information" button →

> The HR manager is taken to the page to update employee's address, telephone number, marital status, dependants, academic record, financial record and criminal record. The modified information is saved in the system database when the "Update" button is clicked.

Add New Employee

If a new employee is recruited, a human resource manager clicks "Add New Employee" button →

> The HR manager is taken to the page to add a new employee's name, employee ID, date of birth, national identification number, address, designation / title, date of recruitment and clearance level. When the "Save" button is clicked, this information is saved to the system database.

Request and View Behavioural Profiles and Security Education and Training Schedules

A security manager or the ISO selects an employee from a drop down box and clicks "Request Behavioural Profiles" button →

A summary of the behavioural patterns and the profile of the selected employee is displayed.

A security manager or ISO clicks "Details" button →

A page containing the detailed behavioural profile is displayed.

A security manager or ISO clicks "Graphs" button →

A page containing graphs and charts displays the behavioural profile graphically.

A security manager or ISO clicks "Training Schedules" button →

A page depicting schedules of the security awareness training required by the employee graphically on a calendar is displayed.

The ISO clicks "Separate Views" button →

A page separating cyber activities of the employee, personal views of their managers or security personnel on non-cyber activities, and background information, into different categories is displayed to allow the ISO to recognize personal biases against the employee.

Emergency Alerts

When a security breach is detected, an emergency pop-up notification immediately alerts the ISO of this breach in real-time, allowing the ISO to take immediate action against the perpetrator and inform relevant authorities.

Configure Security Behavioural Rules

When the ISO clicks “Configure Security Rules” button →

A page containing a table allowing the ISO to configure security behavioural rules to be aligned with the specific requirements of the organization is displayed. Once the ISO makes the necessary configurations and clicks the “Save” button, the new configurations are saved to the rule configuration database to be used for security behavioural profiling.

3.2.3.2 Use Cases

The basic use cases of this system are described in this section. Figure 3.3 and table 3.1 describe the use case for personal observations, while figure 3.4 and table 3.2 describe the use case for action on system output.

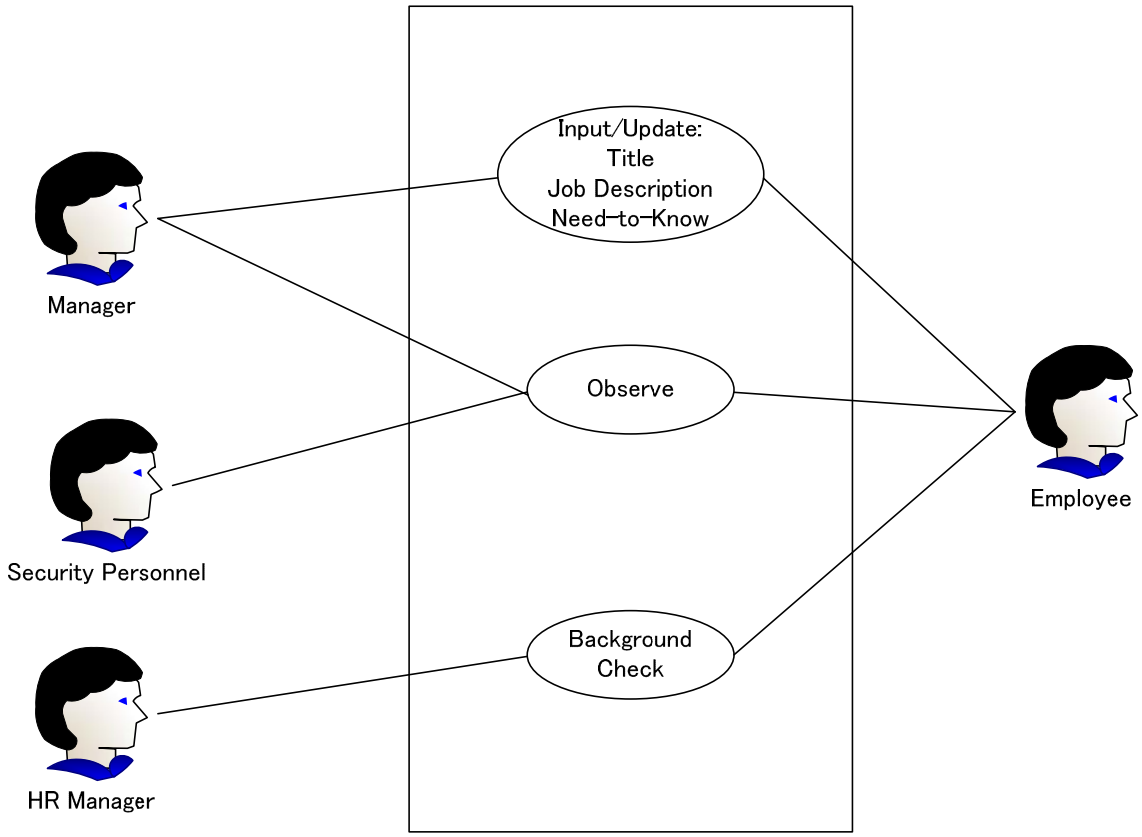

Figure 3.3 – Use Case Diagram for Personal Observations

Table 3.1 – Use Case for Personal Observations

ID	**Personal Observations**
Description	Managers and security personnel observe employees' non-cyber activity and input their observations to the system. Managers also input or update employees' titles, job descriptions and Need-to-Know according to the project(s) the employees are currently working on. Human resource managers input information of background checks carried out on new recruits and update information about current employees after periodic background checks.
Actors	Managers, security personnel, human resource managers and employees
Preconditions	Employee must be assigned a project to update job specification and Need-to-Know. Employee must be promoted in rank to update title.
Basic Steps	Personal observations by managers and security personnel are recorded in the system database. Background information is recorded in the system database.
Alternate Steps	None
Exceptions	None
Basic validation / Rules	Authentication of managers, security personnel and human resource managers will be validated by the system before they are allowed to log in to the system to perform the relevant inputs or updates.
Postconditions	None

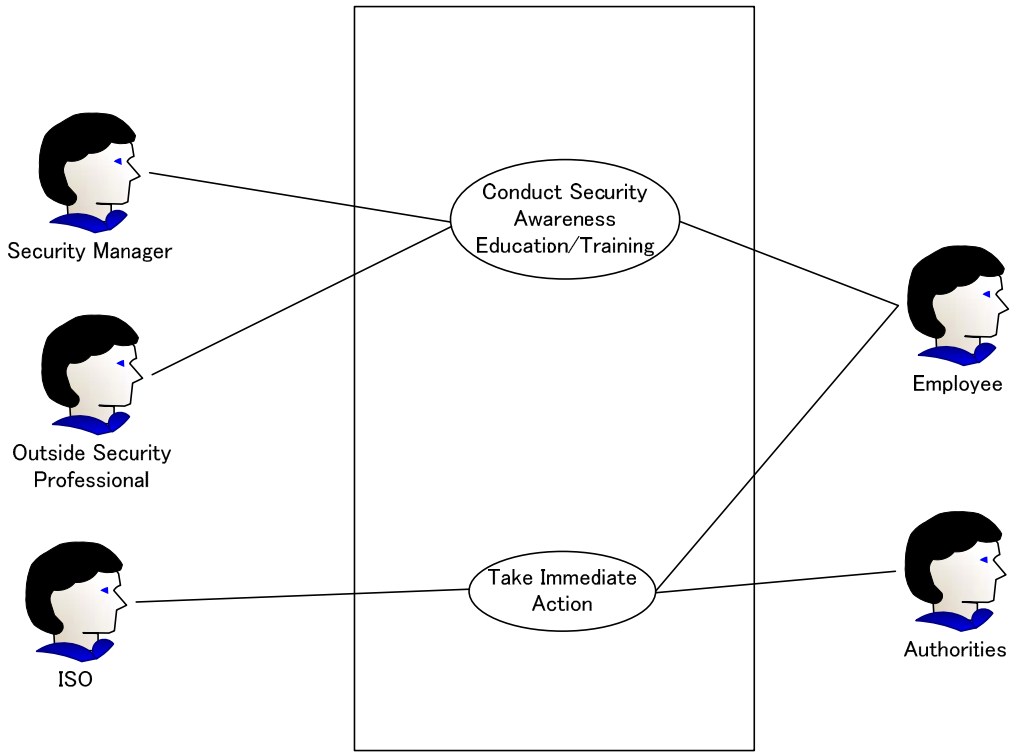

Figure 3.4 – Use Case Diagram for Action on System Output

Table 3.2 – Use Case for Action on System Output

ID	**Action on System Output**
Description	Security managers and external security professionals conduct security awareness education and training programmes as required. Information security officer takes immediate action in the case of an emergency.
Actors	Security managers, security professionals, information security officer, employees and authorities (police, CIA, federal officers etc.)
Preconditions	Employees' cyber activity, non-cyber activity, and background information must be available in the system to compile their security behavioural profiles.
Basic Steps	Security managers obtain output of the system including employees' behavioural profiles and schedules for security training / education and conduct these programmes with outside security professionals.
Alternate Steps	If no training programmes are necessary, the system will provide awareness through automatic pop-up reminders and visual aids.
Exceptions	If an emergency situation is detected, the system alerts the information security officer, who acts immediately to mitigate the problem.
Basic validation / Rules	Authentication of security managers and the information security officer will be validated by the system before they are allowed to log in to the system to perform information retrievals.
Postconditions	None

Chapter 4

Proof of Concept

Chapter 4

Proof of Concept

4.1 Introduction

In order to prove the feasibility of the proposed concept, certain components of this system were implemented during this research. This chapter discusses the design, development and testing of this implemented profiling system.

4.2 System Design

This section discusses the design of this profiling system in detail.

4.2.1 System Database Structure

This system contains two separate databases: one for storing user information and employee behavioural characteristics, and another for configuring security rules of the system, thus allowing these rules to be configured by the ISO to be aligned with the organization's business objectives. The following subsections provide the structure of these databases.

4.2.1.1 Information Security Behavioural Database

Figures 4.1 and 4.2 depict the Entity-Relationship (ER) diagram of the information security behavioural database, and the database schema diagram, respectively.

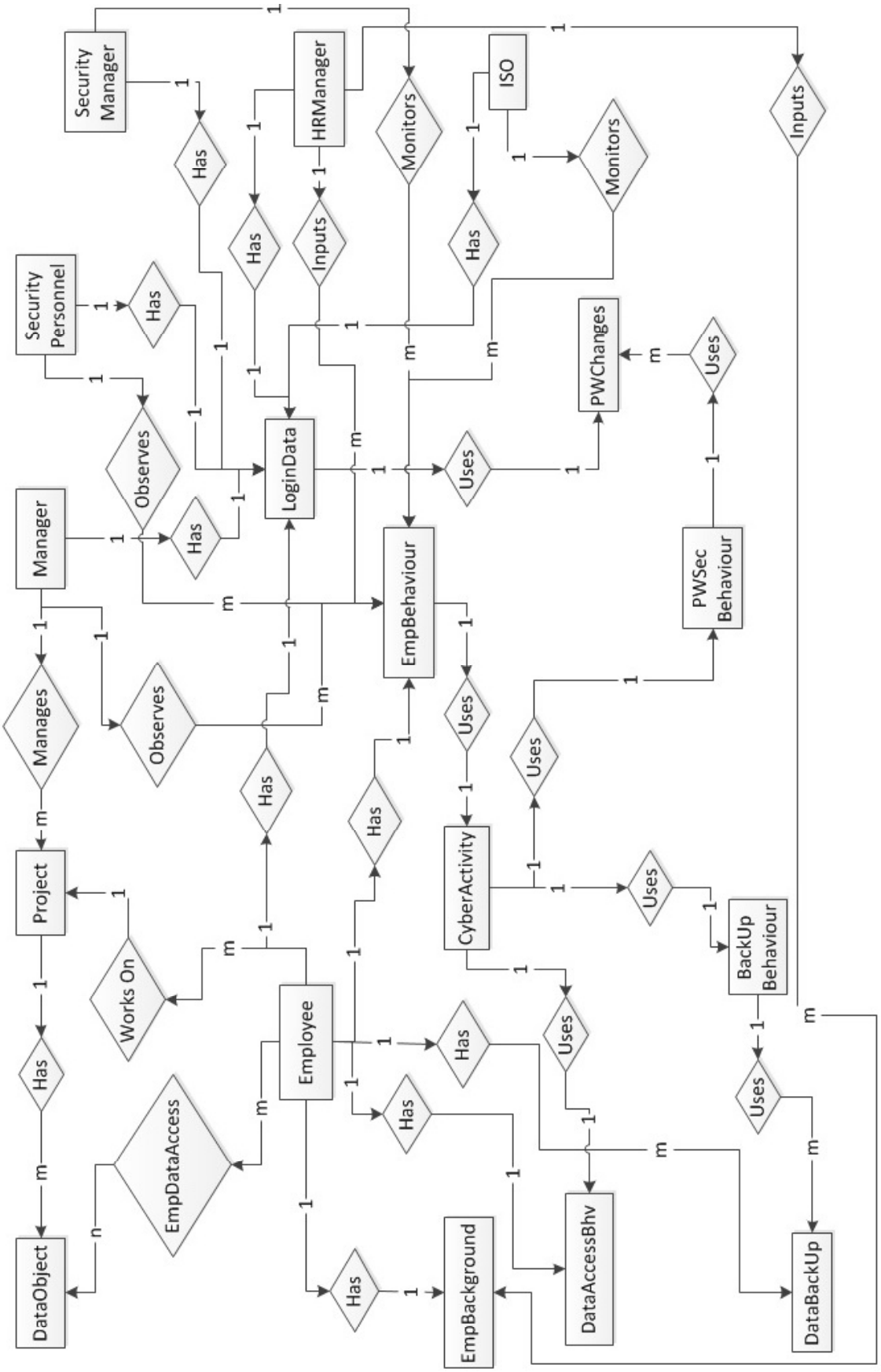

Figure 4.1 – ER Diagram of the Information Security Behavioural Database

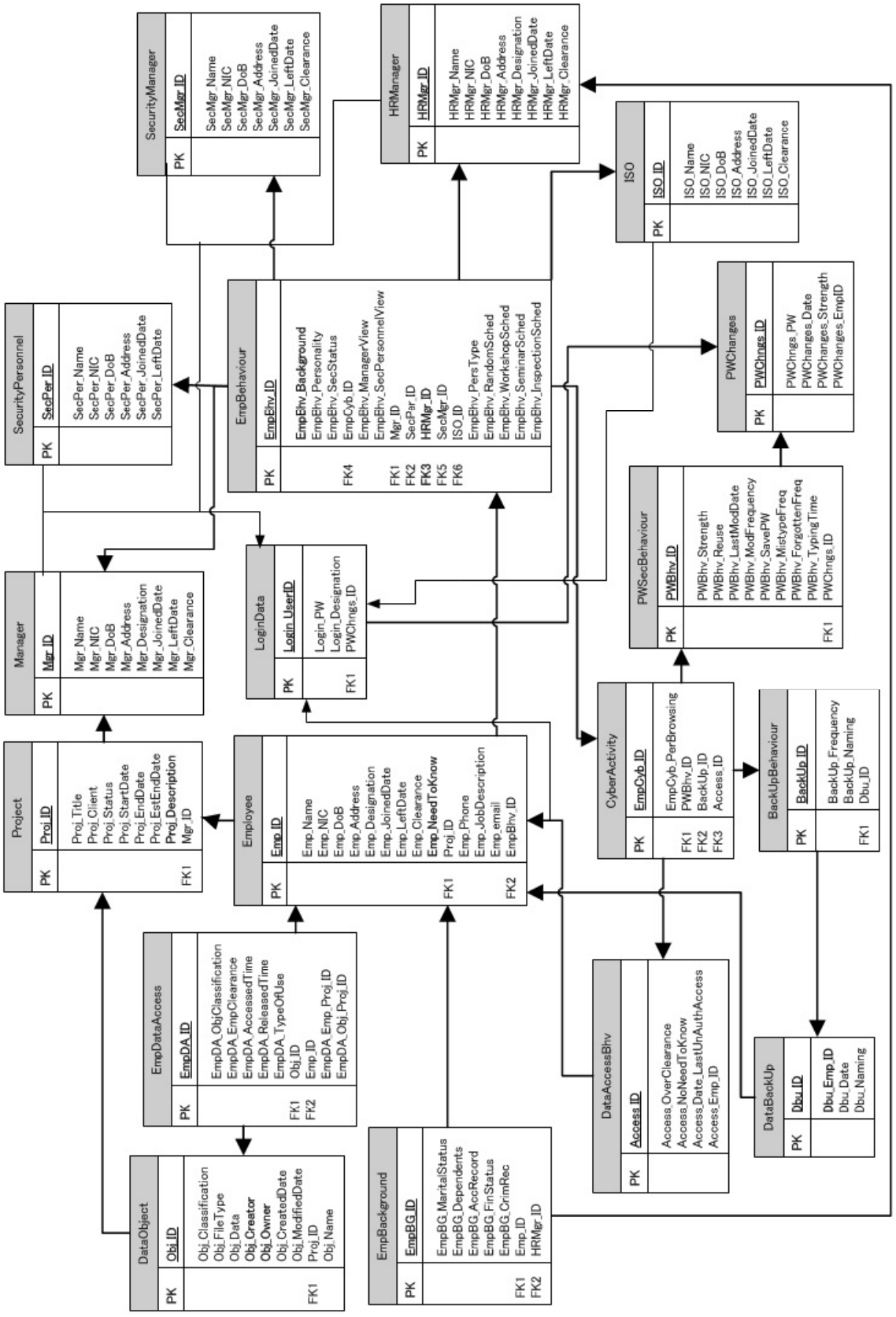

Figure 4.2 – Schema of the Information Security Behavioural Database

4.2.1.2 Information Security Rule Configuration Database

The ER diagram of the security rule configuration database is depicted in figure 4.3.

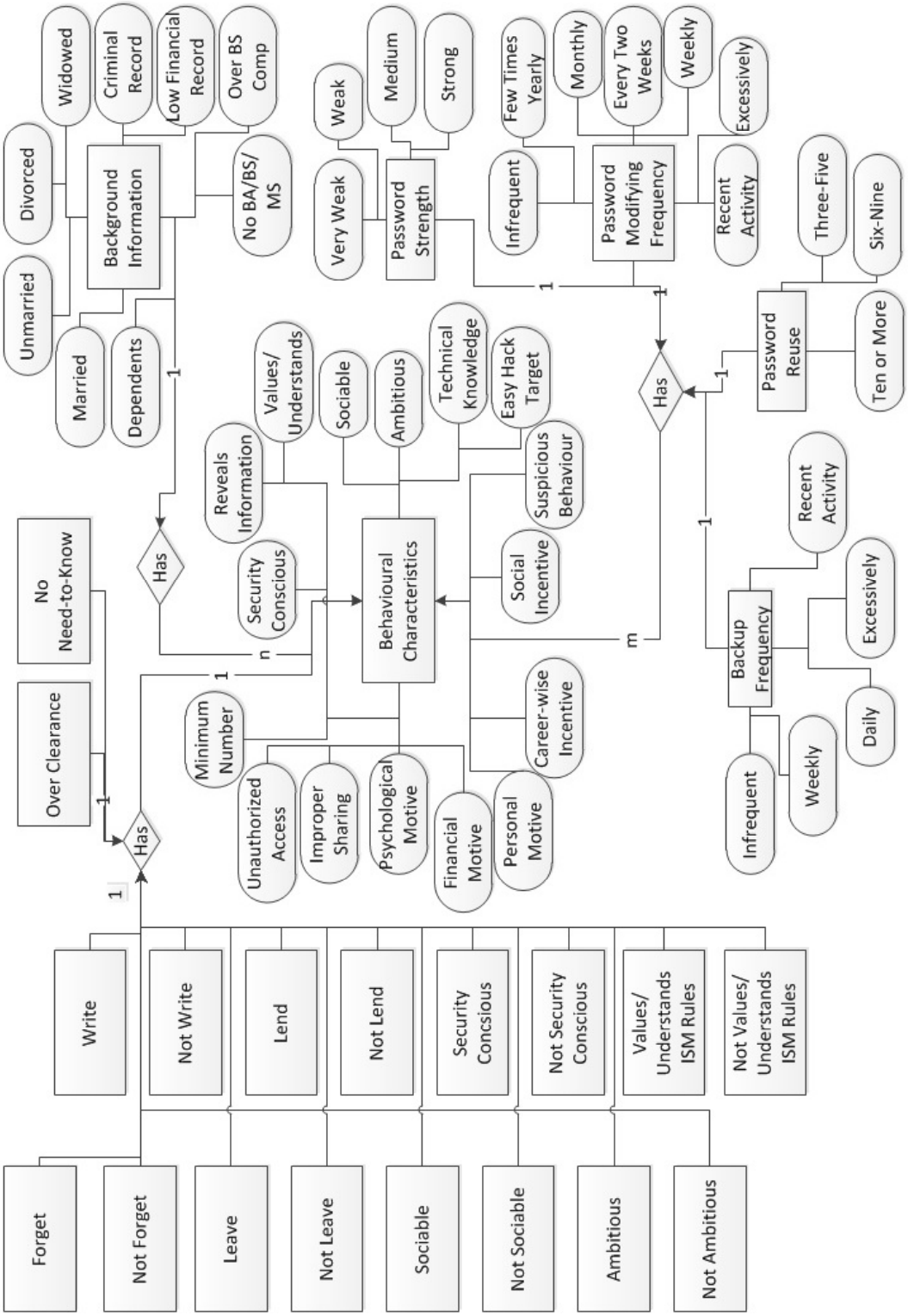

Figure 4.3 – ER Diagram of the Information Security Rule Configuration Database

4.2.2 System Design Diagrams

The activity, sequence, and class diagrams developed during the design phase of this research are examined in this section.

4.2.2.1 Activity Diagrams

The activity diagrams for the user classes of “Employee”, “HR Manager”, “Manager”, “Security Personnel”, “Security Manager” and “Information Security Officer” are depicted in figures 4.4 through 4.9. Figure 4.4 shows how the “Employee” user class may go about their ‘strict mode’ or ‘relaxed mode’ tasks.

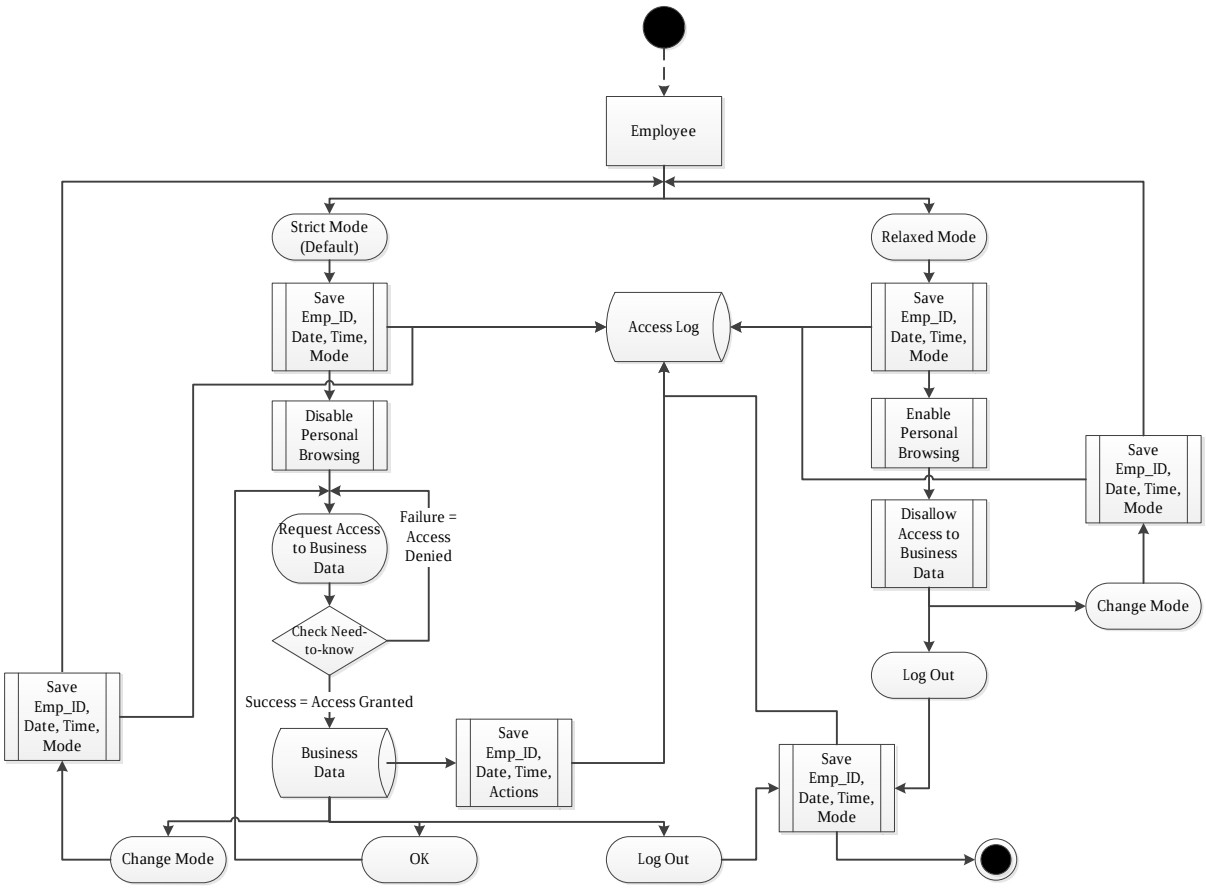

Figure 4.4 – Activity Diagram for the “Employee” User Class

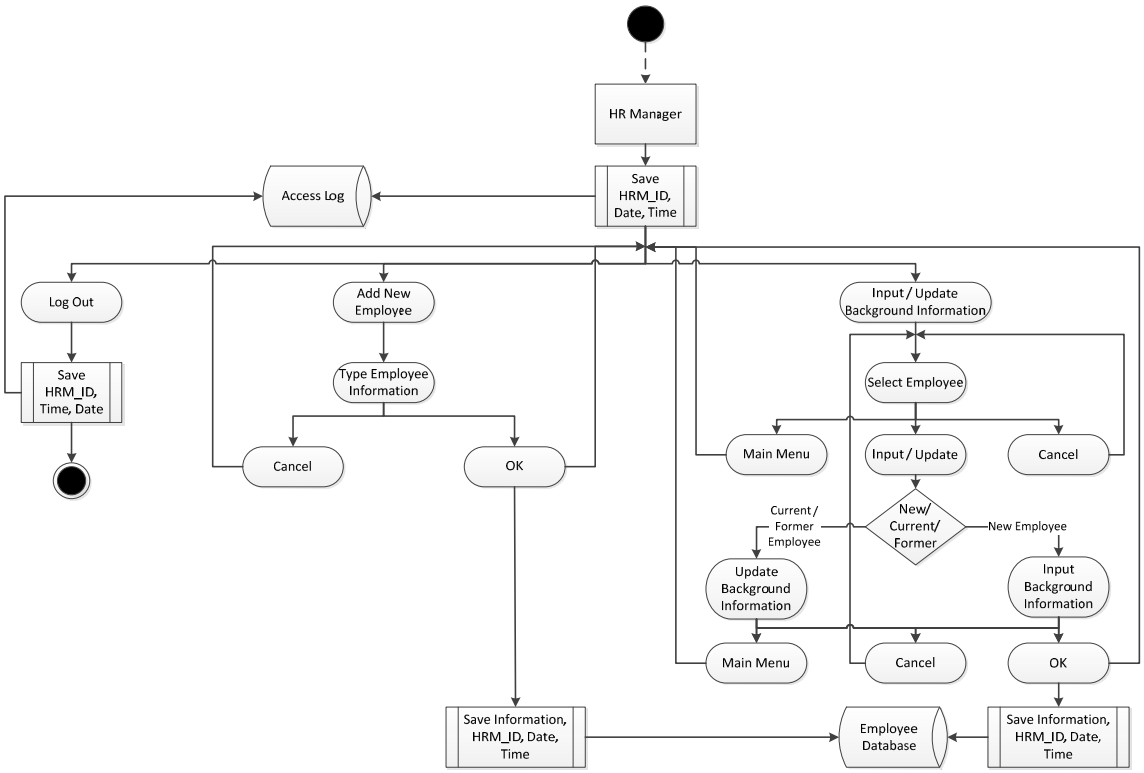

Figure 4.5 – Activity Diagram for the “HR Manager” User Class

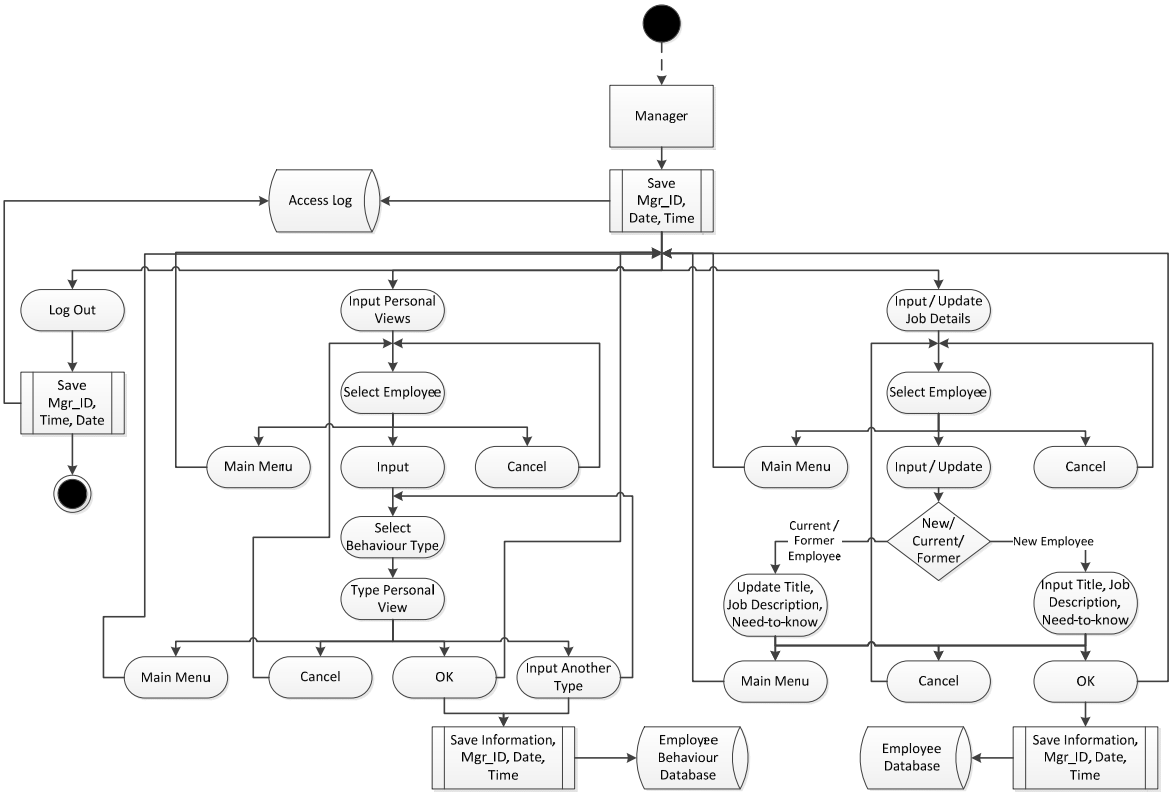

Figure 4.6 – Activity Diagram for the “Manager” User Class

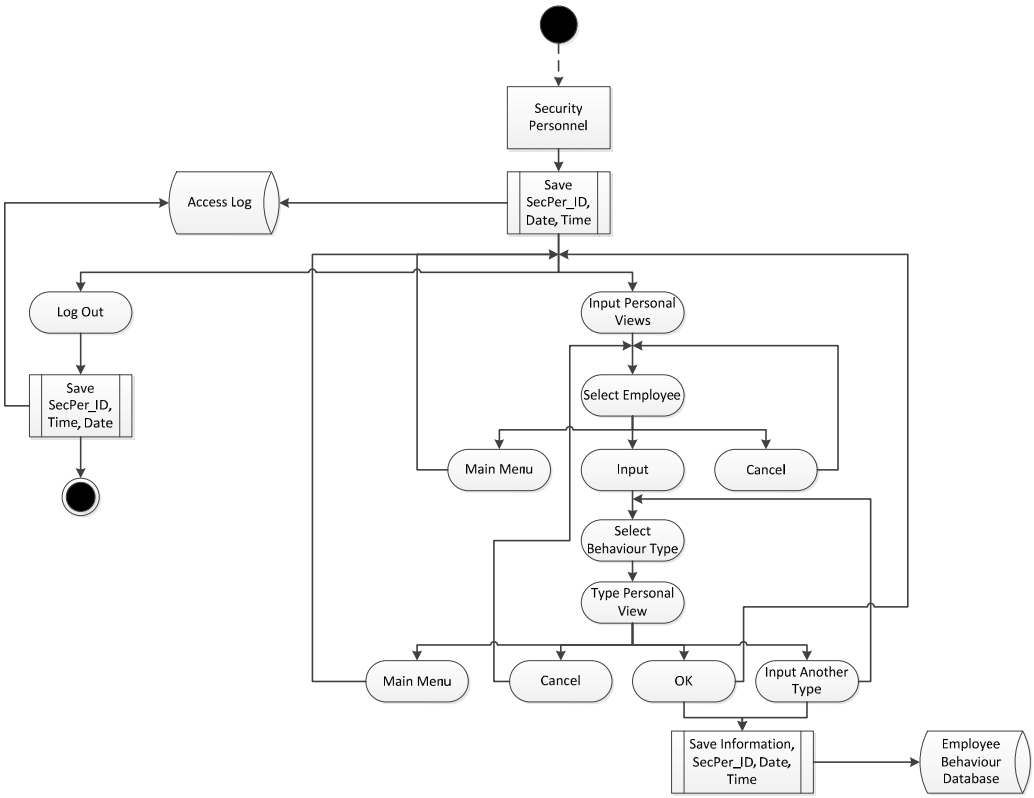

Figure 4.7 – Activity Diagram for the “Security Personnel” User Class

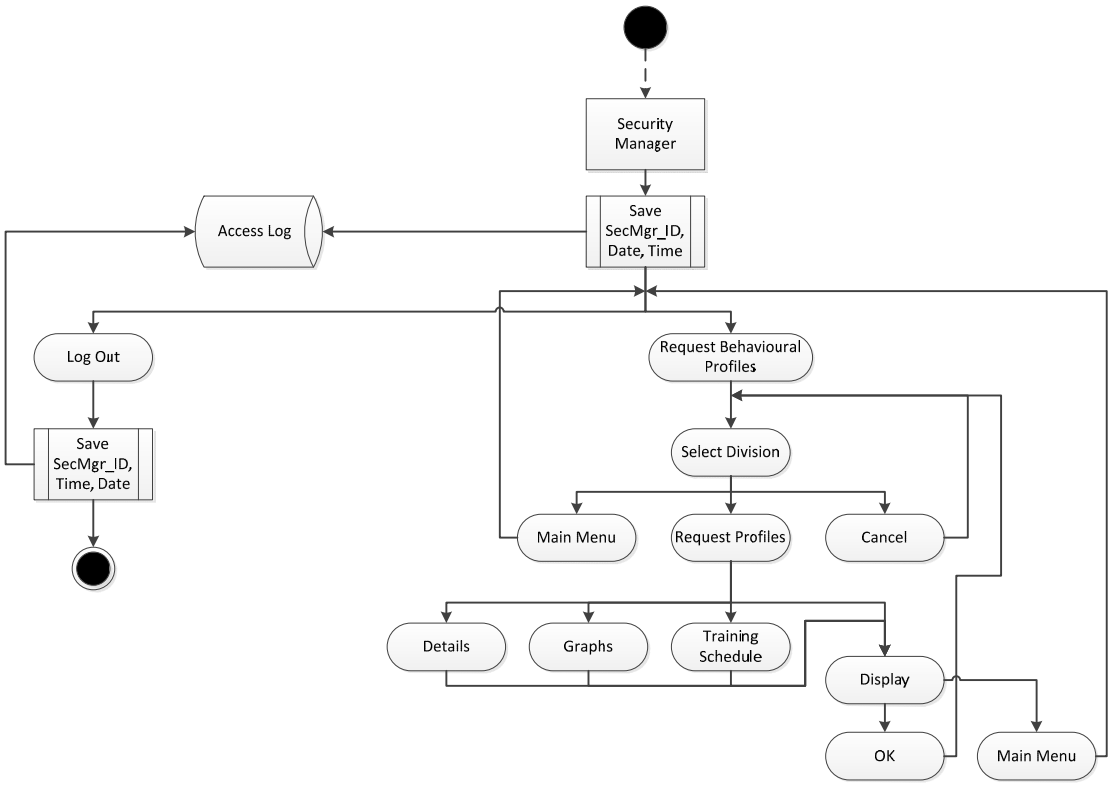

Figure 4.8 – Activity Diagram for the “Security Manager” User Class

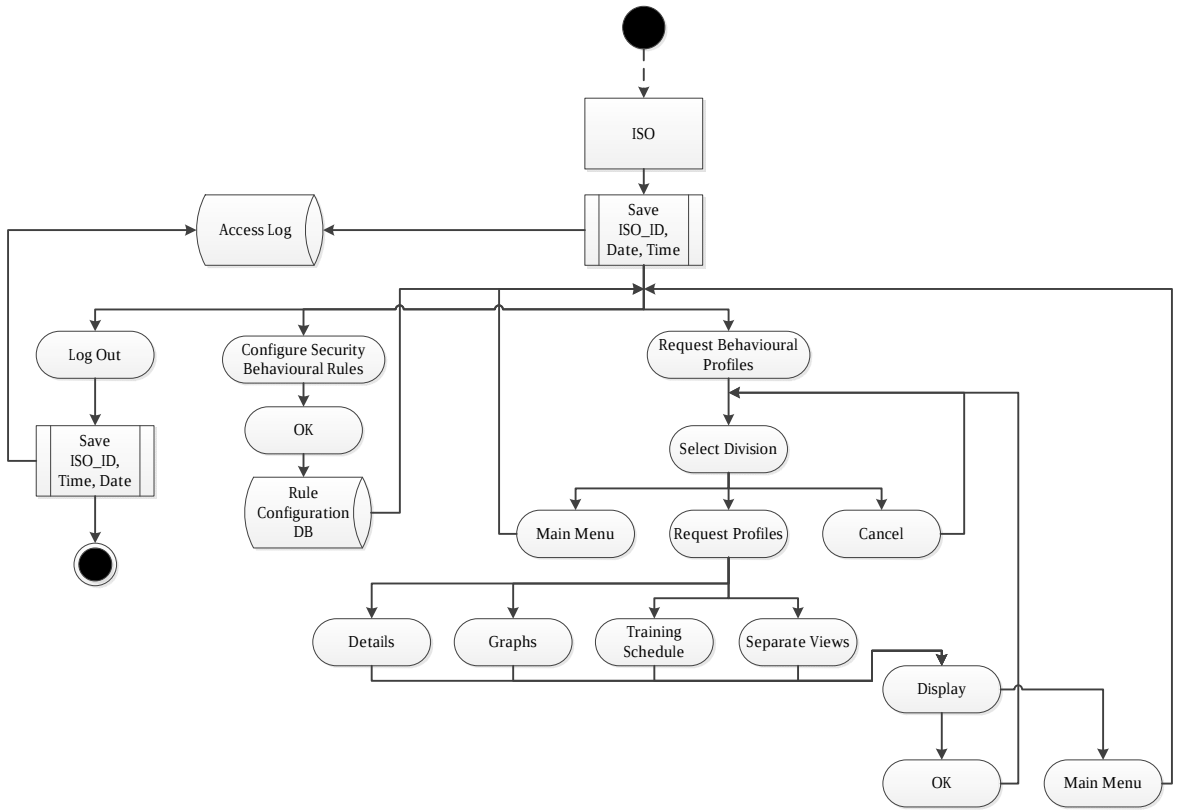

Figure 4.9 – Activity Diagram for the "Information Security Officer" User Class

Figure 4.5 depicts how a human resource manager can add a new employee, or input / update background information, while figure 4.6 shows how a manager may input personal views on an employee's non-cyber activity, or input / update their job descriptions. Figure, 4.7 shows how a security personnel may input their personal views on employees' non-cyber activities, while figure 4.8 shows how a security manager may view summarized, detailed or graphical behavioural profiles and employees' security education and training schedules. Finally, figure 4.9 shows how the information security officer can view summarized, detailed, graphical or separate views of behavioural profiles and employees' security education and training schedules, or configure security behavioural rules.

4.2.2.2 Sequence Diagrams

The sequence diagrams for data access behaviour, password security behaviour, data backup behaviour, data sanitization behaviour, and security behaviour concerning external storage

devices are depicted in figures 4.10 through 4.14. The sequence diagram for viewing security behavioural profiles is depicted in figure 4.15. Figure 4.10 shows how an employee may access data within or below his / her security clearance level and for which they have a Need-to-Know, or how if either condition fails, their profile will be updated with the unauthorized access attempt. Figure 4.11 depicts how profiles are updated with password strength, modifying frequency, reuse of former passwords, and mistyping of passwords, while figure 4.12 shows updating profiles with data backup frequency and the following of backup naming conventions etc. Figures 4.13 and 4.14 depict the updating of profiles for data sanitization, scanning and validating external storage media, while figure 4.15 shows the process of requesting to view security behavioural profiles by the ISO / security managers.

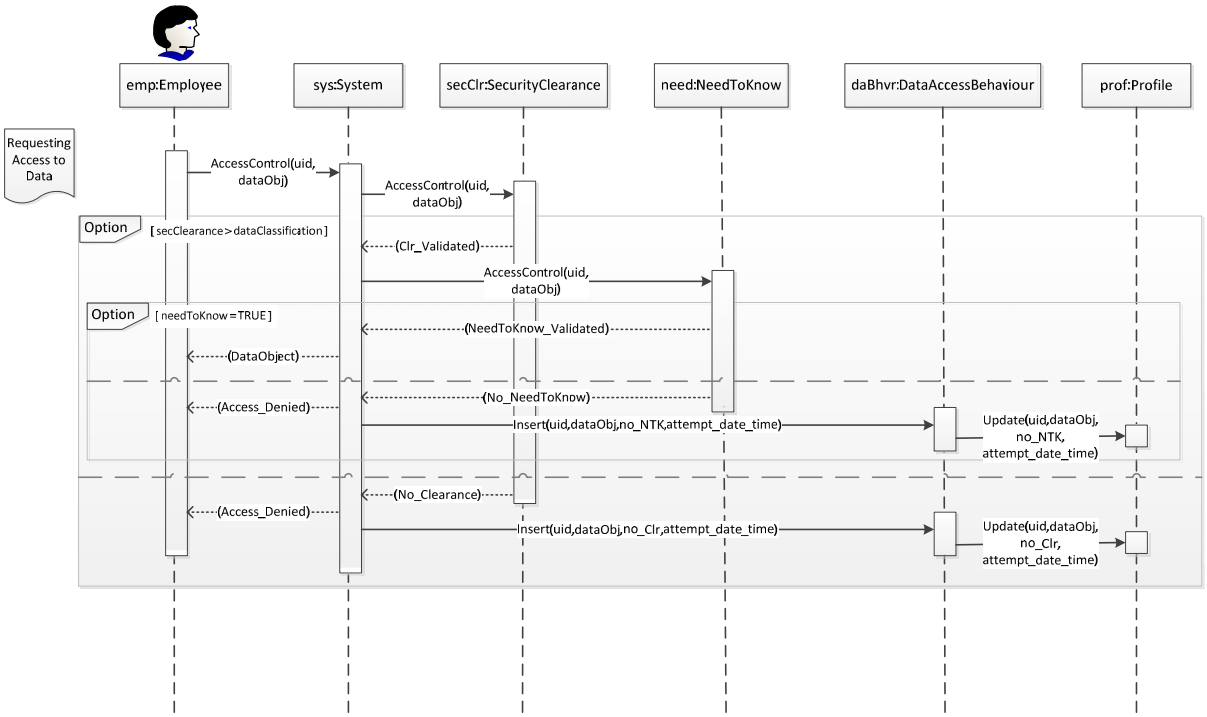

Figure 4.10 – Sequence Diagram for Data Access Behaviour

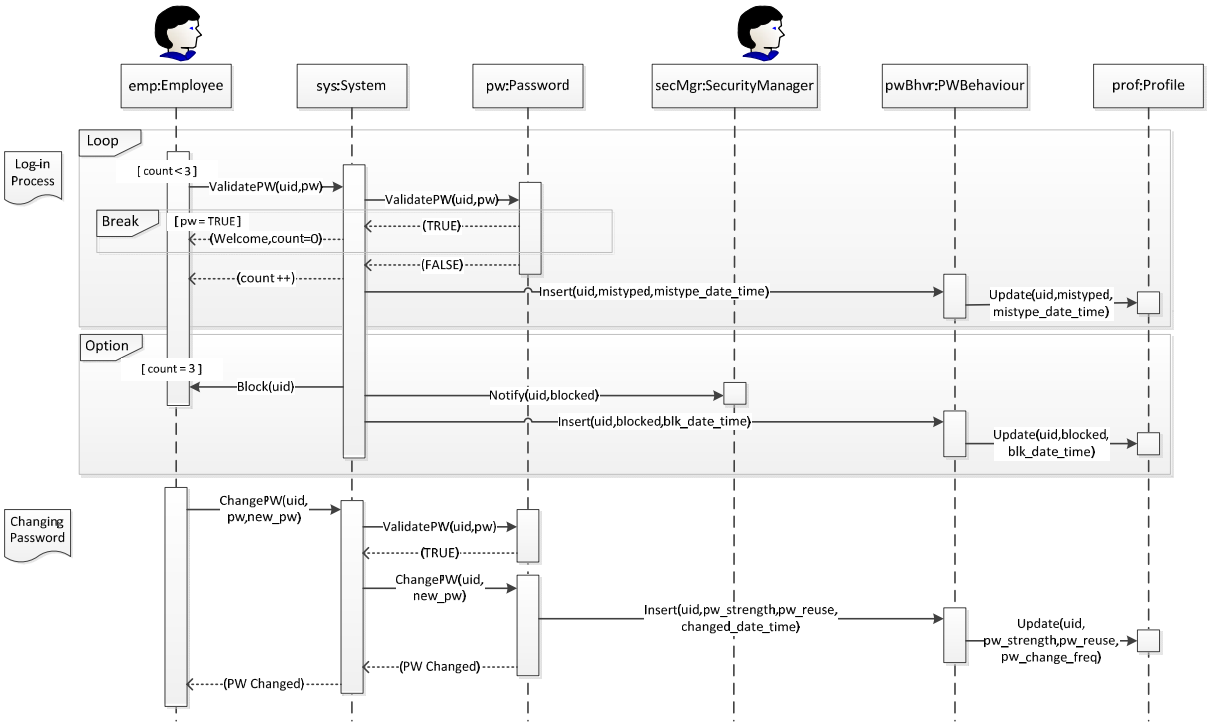

Figure 4.11 – Sequence Diagram for Password Security Behaviour

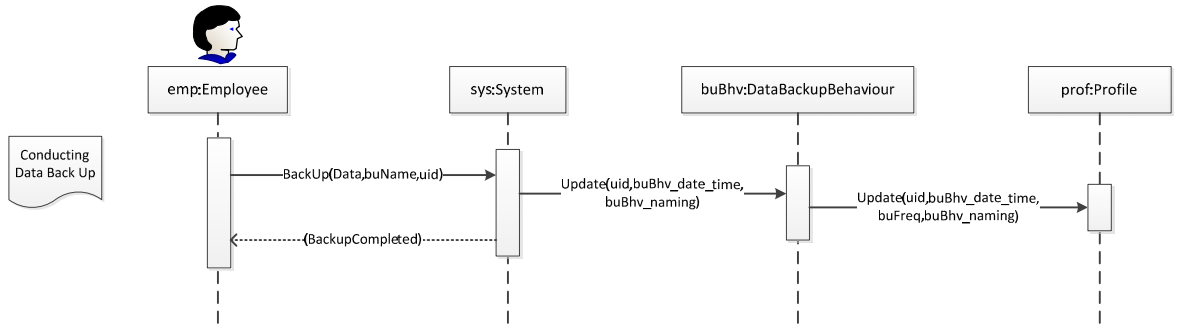

Figure 4.12 – Sequence Diagram for Data Backup Behaviour

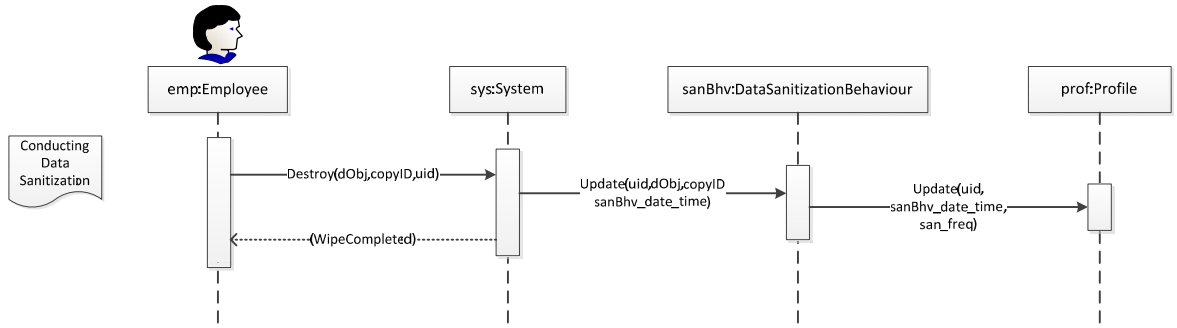

Figure 4.13 – Sequence Diagram for Data Sanitization Behaviour

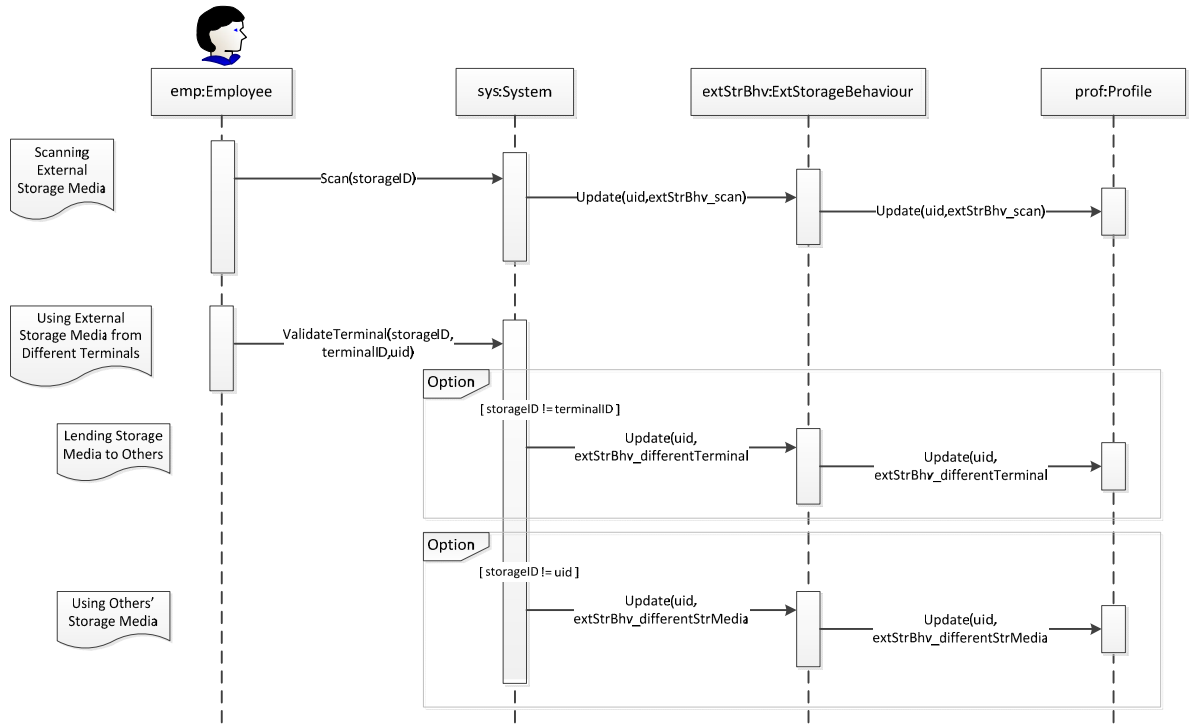

Figure 4.14 – Sequence Diagram for Security Behaviour concerning External Storage Devices

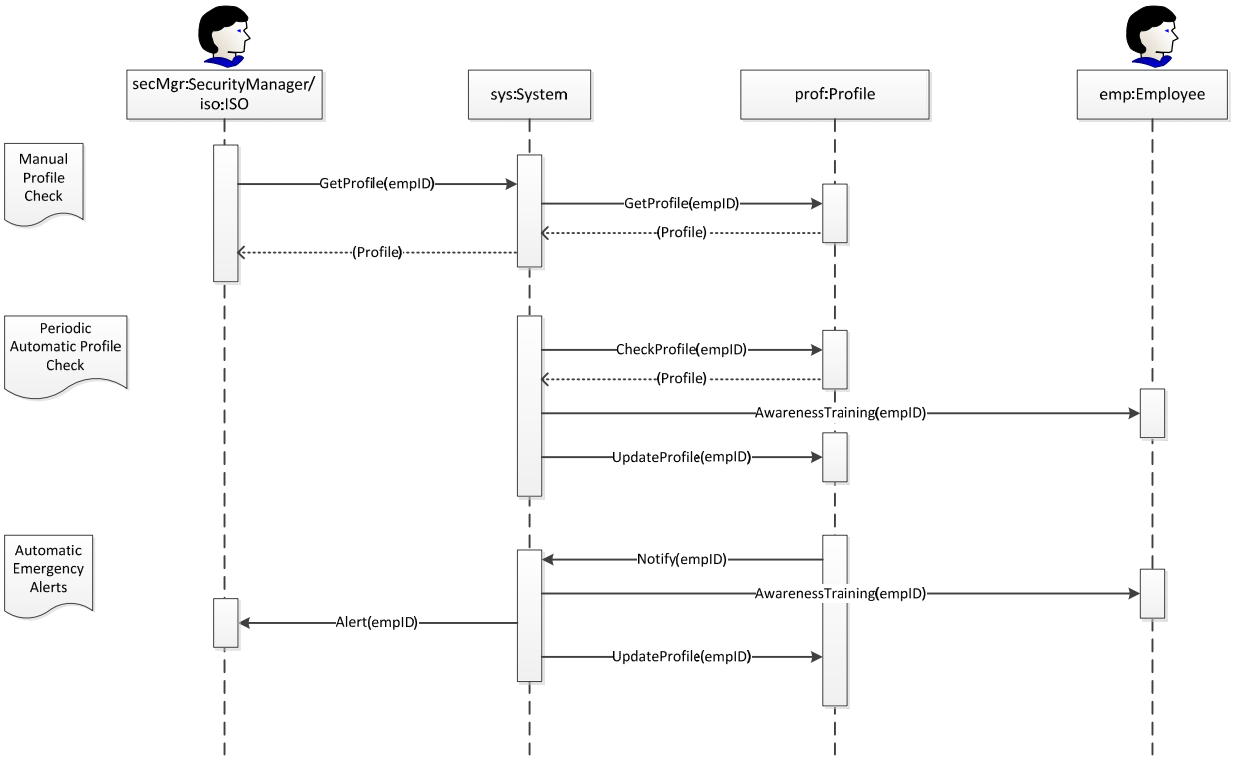

Figure 4.15 – Sequence Diagram for Viewing Security Behavioural Profiles

4.2.2.3 Class Diagrams

The basic class diagram of the security behavioural profiling system is depicted in figure 4.16.

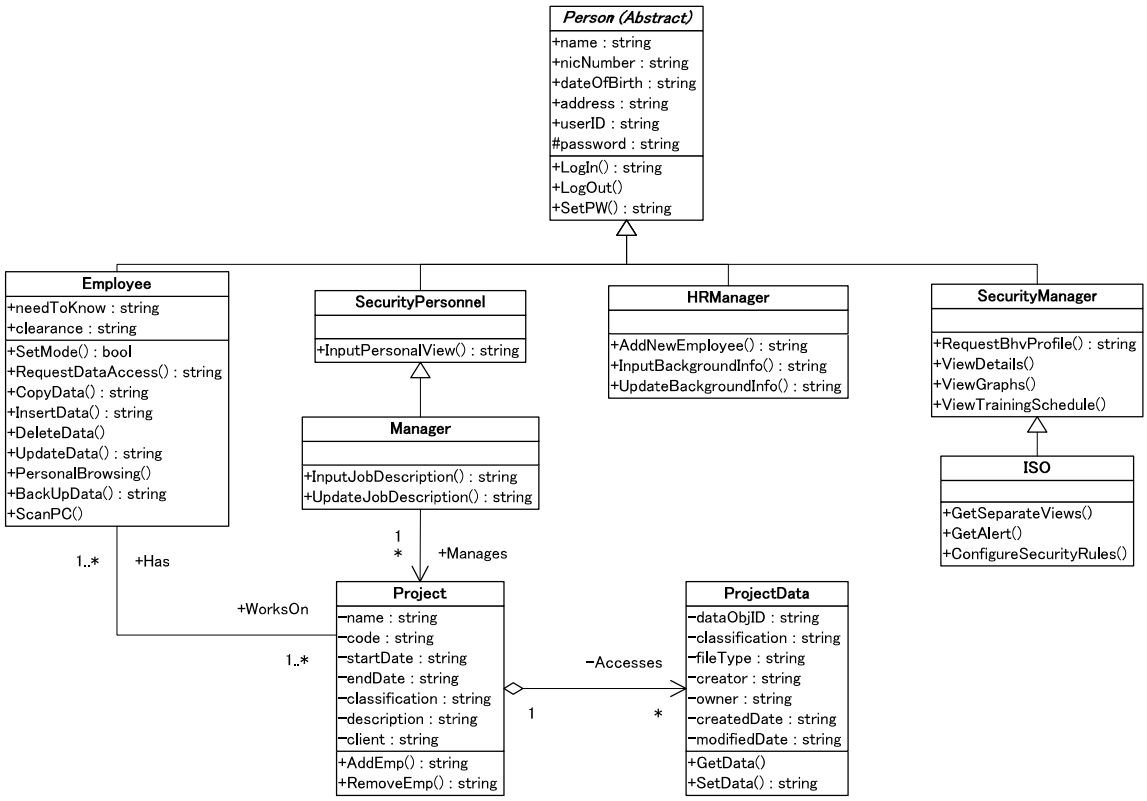

Figure 4.16 – Class Diagram of the Security Behavioural Profiling System

As can be seen through figure 4.16, the “Manager” user class has all the functionality a “Security Personnel” user class possesses concerning inputting personal views on non-cyber behaviour of employees, in addition to the functionality of inputting / updating job descriptions. Similarly, the “ISO” user class possesses all the functionality the “Security Manager” user class has of viewing behavioural profiles in summarized, detailed and graphical views and viewing employees’ security education and training schedules, in addition to being able to view behavioural profile components separately, receive emergency alerts concerning extremely problematic behaviour, as well as being able to configure the security behavioural rules to be aligned with the business objectives of the organization.

4.3 System Development

This section discusses the aspects of implementation of the security behavioural profiling system. Both the front-end and the back-end of the system were developed on NetBeans Integrated Development Environment (IDE) 7.4 platform, using Java Development Kit (jdk1.7.0).

4.3.1 Database Development

The databases of the behavioural profiling system (both the information security behavioural database and the security rule configuration database) were developed on pgAdmin III v1.14.3 using PostGreSQL and java database connectivity (JDBC).

4.3.2 Front-End Development

The development of the graphical user interfaces (GUIs) of the front-end of the system are discussed in the subsequent subsections. In addition to the basic components of jdk1.7.0, the front-end development of this system also required the use of jfreechart-1.0.16 and jcalendar components.

4.3.2.1 Graphical User Interfaces for "Employee"

The GUIs depicting employees' tasks, employees' strict mode tasks, changing password and accessing data are depicted in figures 4.17 through 4.20.

Figure 4.17 – Employees' Tasks GUI

Figure 4.18 – Employees' Strict Mode Tasks GUI

Figure 4.19 – GUI for Changing Password

Figure 4.20 – GUI for Accessing Data

4.3.2.2 Graphical User Interfaces for "Human Resource Manager"

The GUI depicting HR managers' tasks, the GUI for adding a new employee, the GUI for selecting an employee for updating background information, and the GUI for inputting or updating employee's background information, respectively, are depicted in figures 4.21 through 4.24.

Figure 4.21 – HR Managers' Tasks GUI

Figure 4.22 – GUI for Adding a New Employee

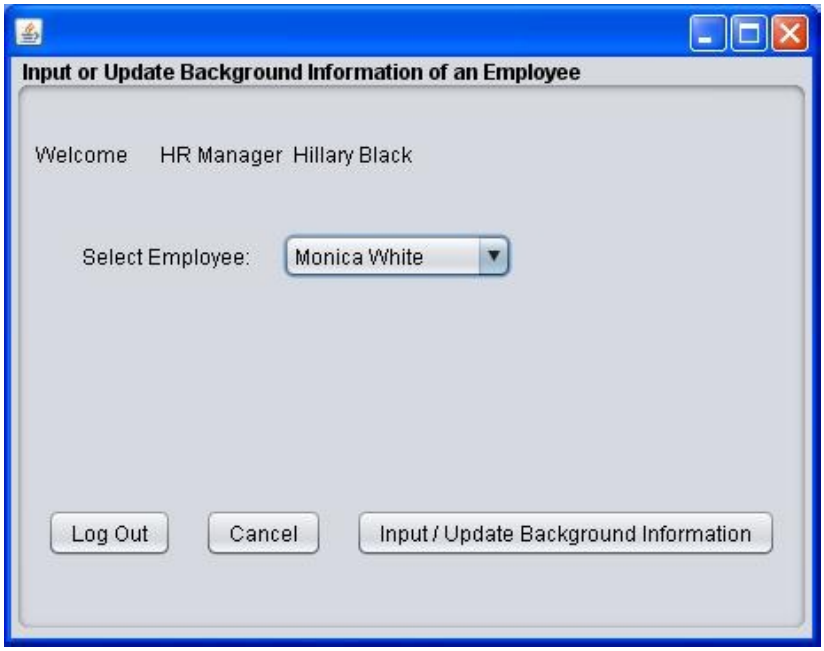

Figure 4.23 – GUI for Selecting an Employee to Update Background Information

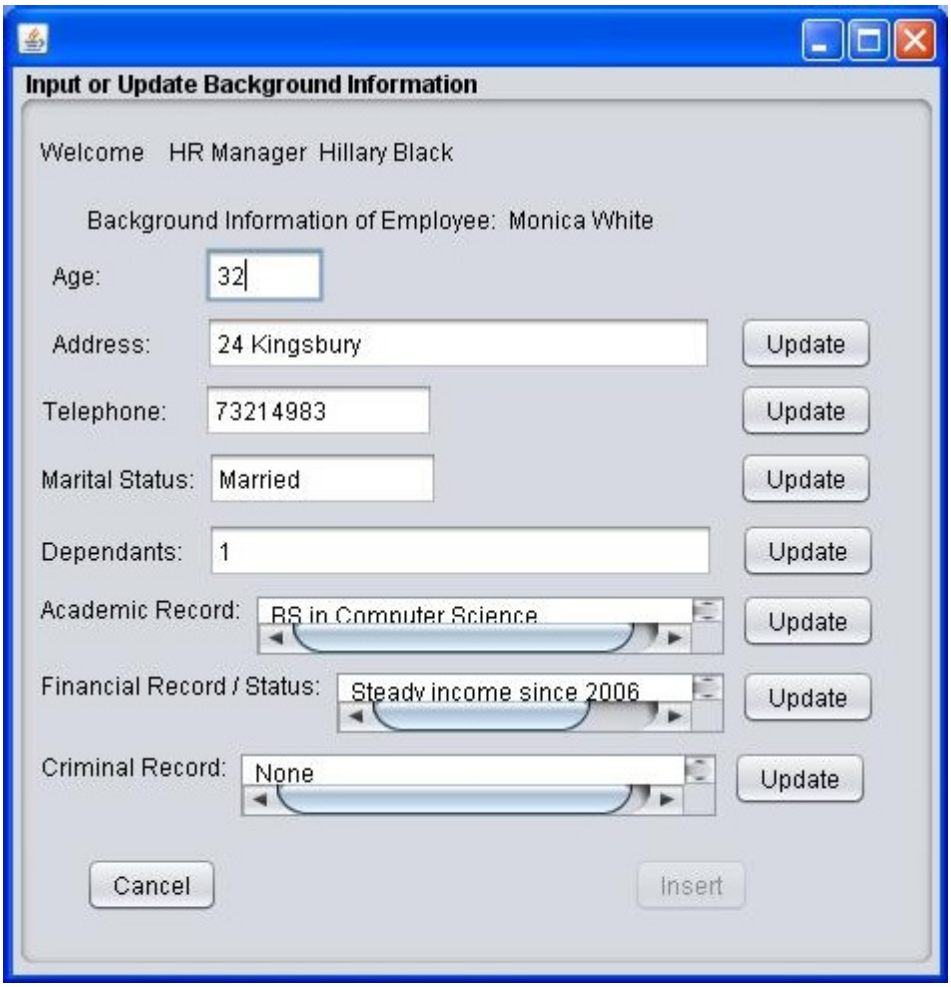

Figure 4.24 – GUI for Inputting / Updating Employee Background Information

4.3.2.3 Graphical User Interfaces for "Manager"

The GUI depicting Managers' tasks, the GUI for selecting an employee to update job details, and the GUI for updating employee job details are depicted in figures 4.25 though 4.27. The GUIs for allowing managers to select an employee to input his personal view about the employee's security behaviour, and for inputting his personal view, are similar to the GUIs allowing the security personnel to do the same, and thus, are discussed under activities of security personnel.

Figure 4.25 – Managers' Tasks GUI

Figure 4.26 – GUI for Selecting Employee to Update Job Details

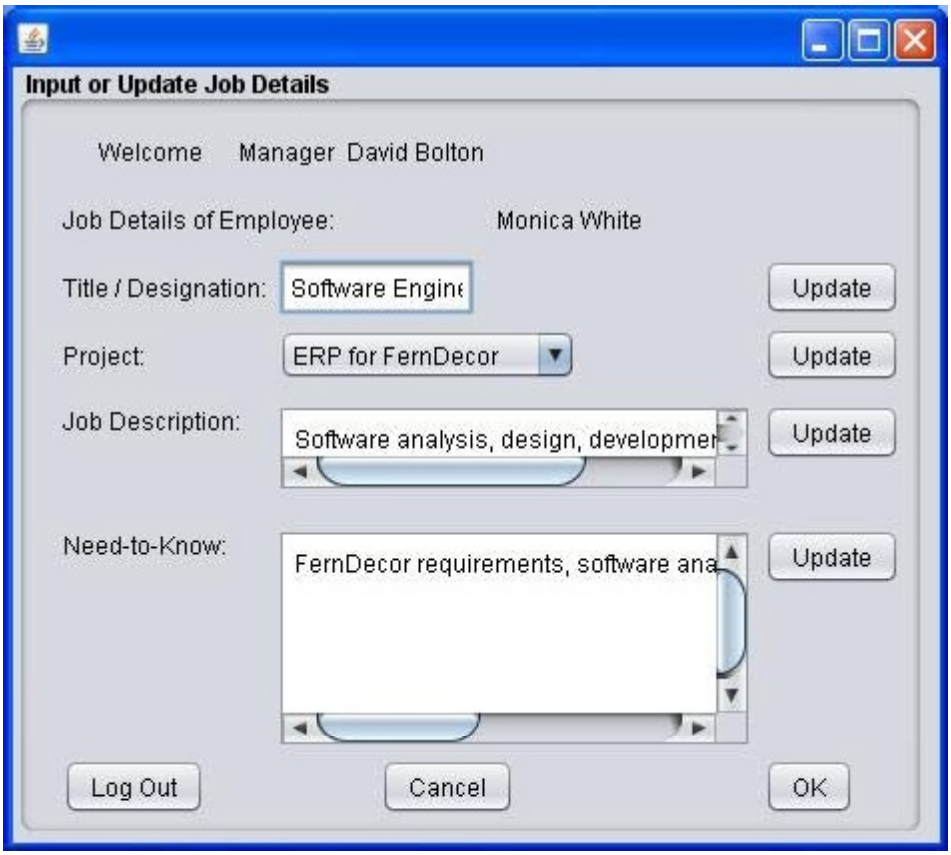

Figure 4.27 – GUI for Inputting / Updating Employee Job Details

4.3.2.4 Graphical User Interfaces for "Security Personnel"

The GUIs allowing a security personnel to select an employee to input his personal view about the employee's security behaviour, and for inputting his personal view, are depicted through figures 4.28 and 4.29, respectively.

Figure 4.28 – GUI for Selecting Employee to Input Personal Views of Security Behaviour

Figure 4.29 – GUI for Inputting Personal Views on Employee's Security Behaviour

4.3.2.5 Graphical User Interfaces for "Security Manager"

The GUIs allowing a security manager to request security behavioural profiles and view the summarized profile are depicted in figures 4.30 and 4.31, respectively. The GUIs allowing security managers to view detailed and graphical profiles, and to view security training schedules are similar to the GUIs allowing the ISO to do the same, and thus are discussed under activities of the ISO.

Figure 4.30 – GUI for Requesting Security Behavioural Profiles

Figure 4.31 – GUI for Viewing a Summarized Profile by a Security Manager

4.3.2.6 Graphical User Interfaces for "Information Security Officer"

The GUI depicting the ISO's tasks is shown in figure 4.32. The GUIs allowing the ISO to view security behavioural profiles in summarized, detailed, and graphical form, and as separate views are depicted in figures 4.33 through 4.36, respectively, while figure 4.37 depicts the GUI for viewing security education and training schedules. The GUI depicting the requesting to view security profiles by the ISO is similar to that allowing the security managers to do the same as discussed in the previous subsection. Figure 4.38 depicts the GUI for configuring security rules.

Figure 4.32 – ISO's Tasks GUI

Figure 4.33 – GUI for Viewing a Summarized Profile by the ISO

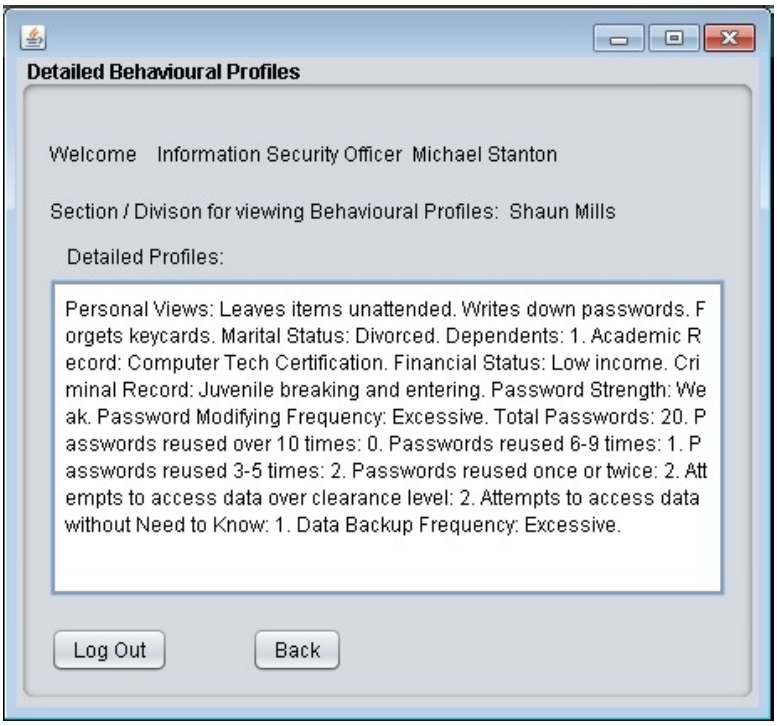

Figure 4.34 – GUI for Viewing a Detailed Profile by the ISO

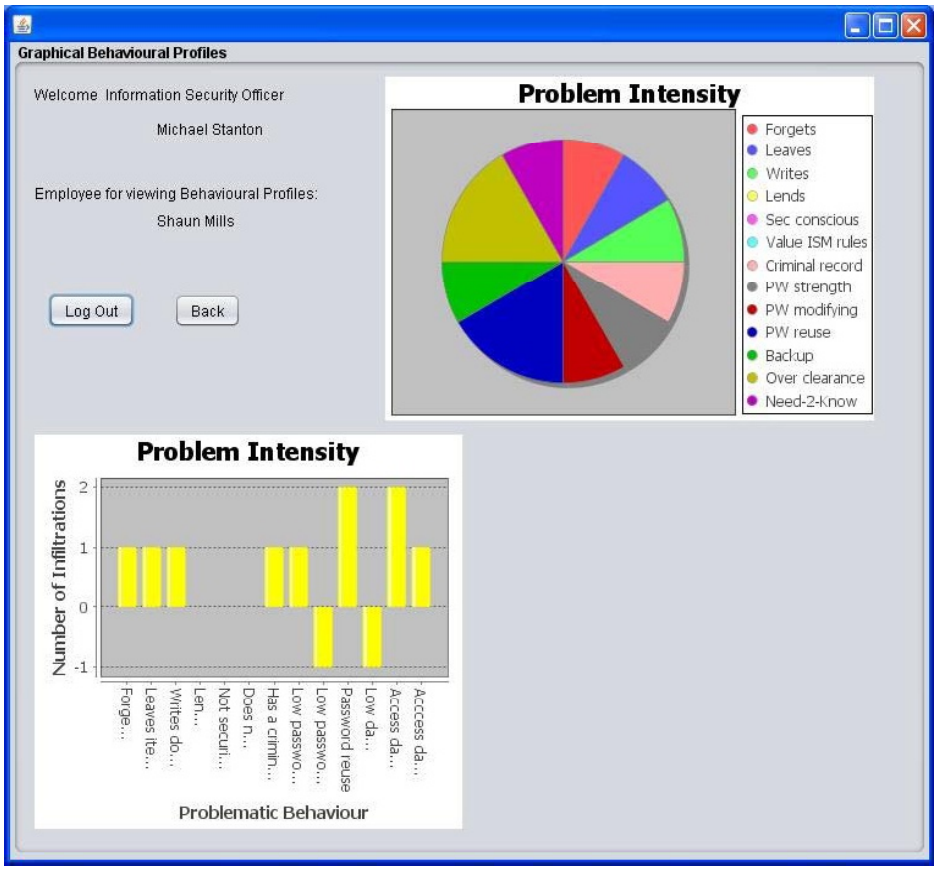

Figure 4.35 – GUI for Viewing a Graphical Profile by the ISO

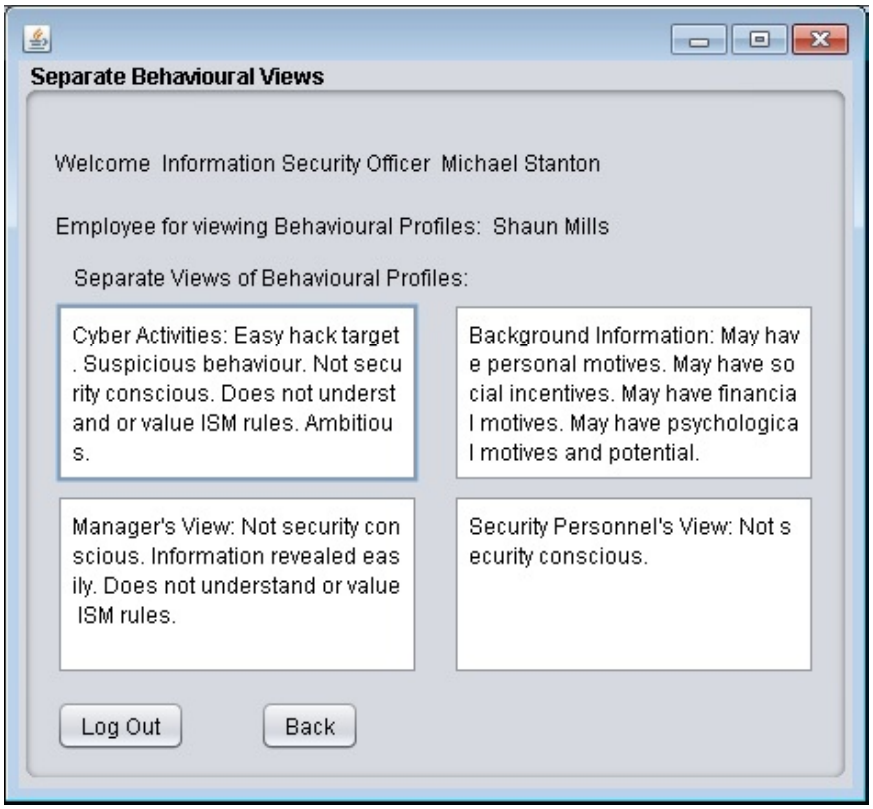

Figure 4.36 – GUI for Viewing a Profile as Separate Views by the ISO

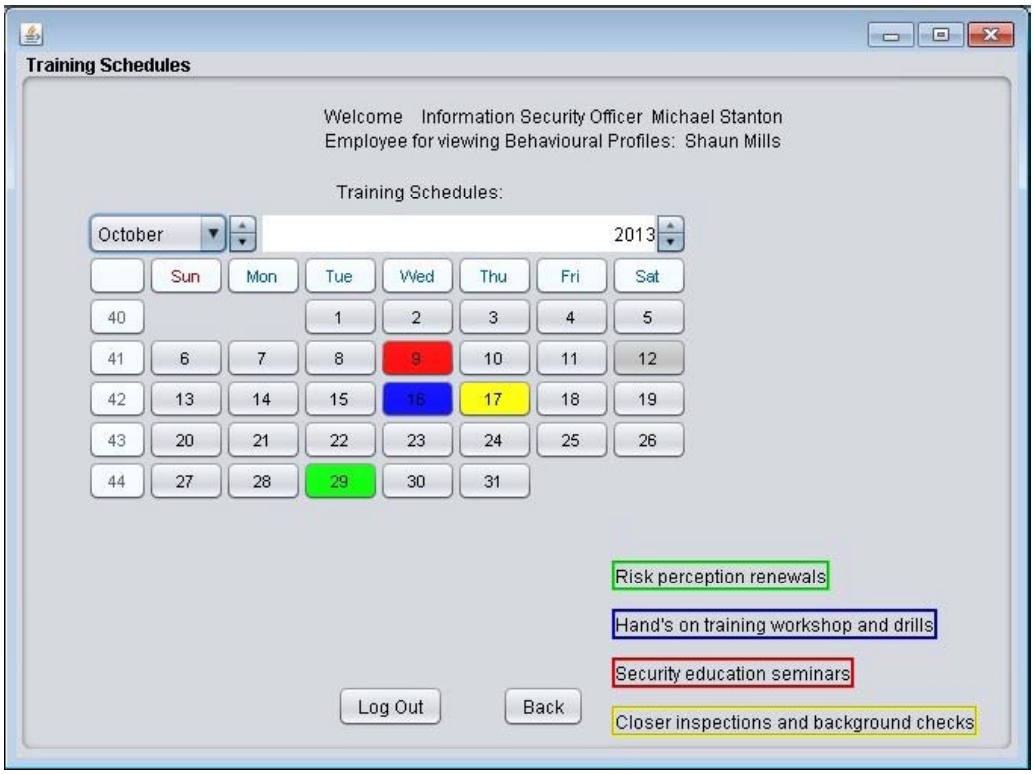

Figure 4.37 – GUI for Viewing a Security Education and Training Schedule

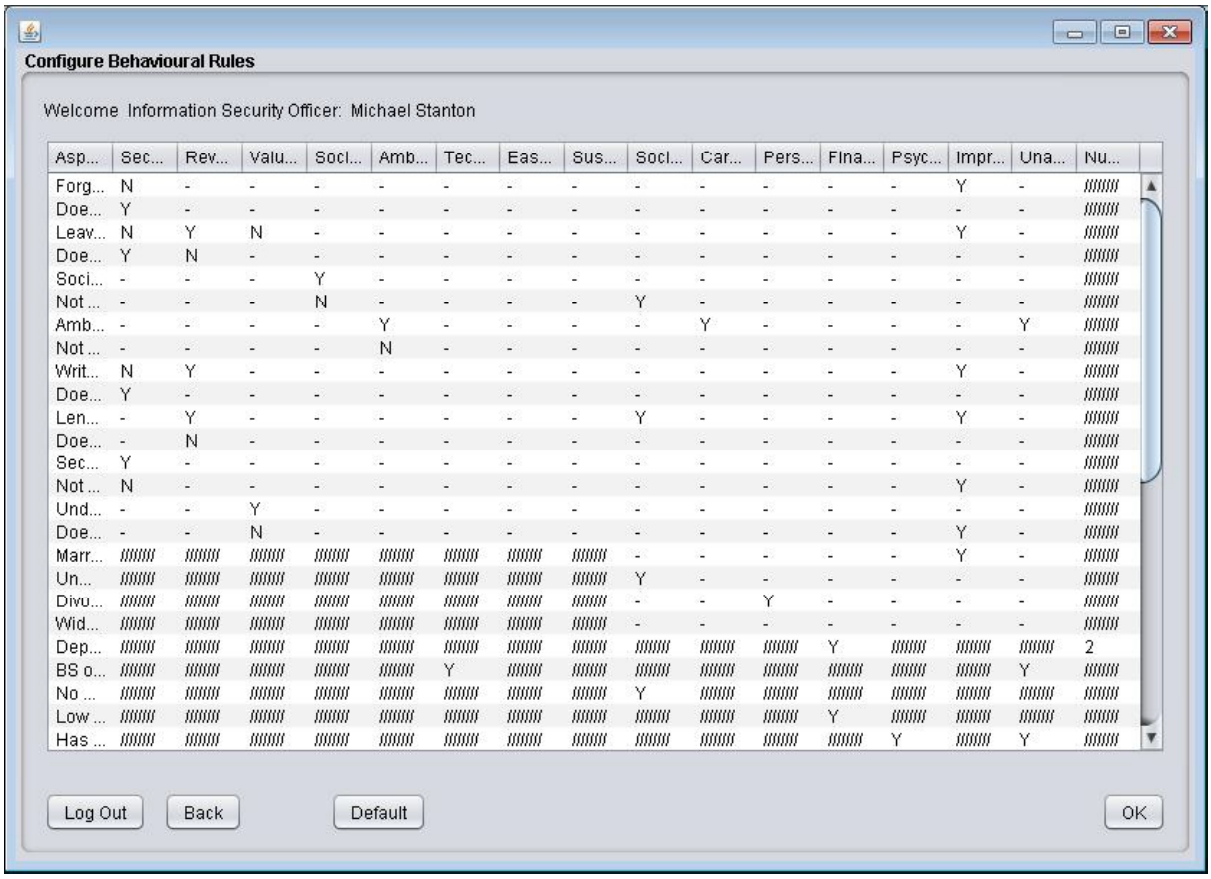

Figure 4.38 – GUI for Configuring Security Behavioural Rules

4.3.3 Back-End Development

Since programs to detect various aspects of data sanitization behaviour and network security behaviour are currently available, this system implementation focuses mainly on the monitoring of password security behaviour, data backup behaviour, and physical security behaviour. The following aspects of this system were implemented and tested through this research:

- *Strict mode*
- *Password Security Behaviour*: password strength (an existing common algorithm was reused), password modifying frequency, password reuse
- *Data Access and Backup Behaviour*: data backup frequency, attempts to access data over clearance, attempts to access data without need to know

- *Personal observations*: forgetting keycards or Personal Identification Numbers (PINs), leaving items unattended, sociability, ambitiousness, writing passwords down, lending keycards or PINs, security consciousness, understanding and valuing ISM rules
- *Information obtained through background checks*: marital status, number of dependents, academic record, financial status record, criminal record
- *Configuration of security behavioural rules*
- *Creation of user security behavioural profiles*: displayed in summarized, detailed, and graphical versions, and as separate views
- *Scheduling security awareness, education and training*

The architecture of the developed system is depicted in figure 4.39. Each of these areas will be examined in detail in the rest of this section.

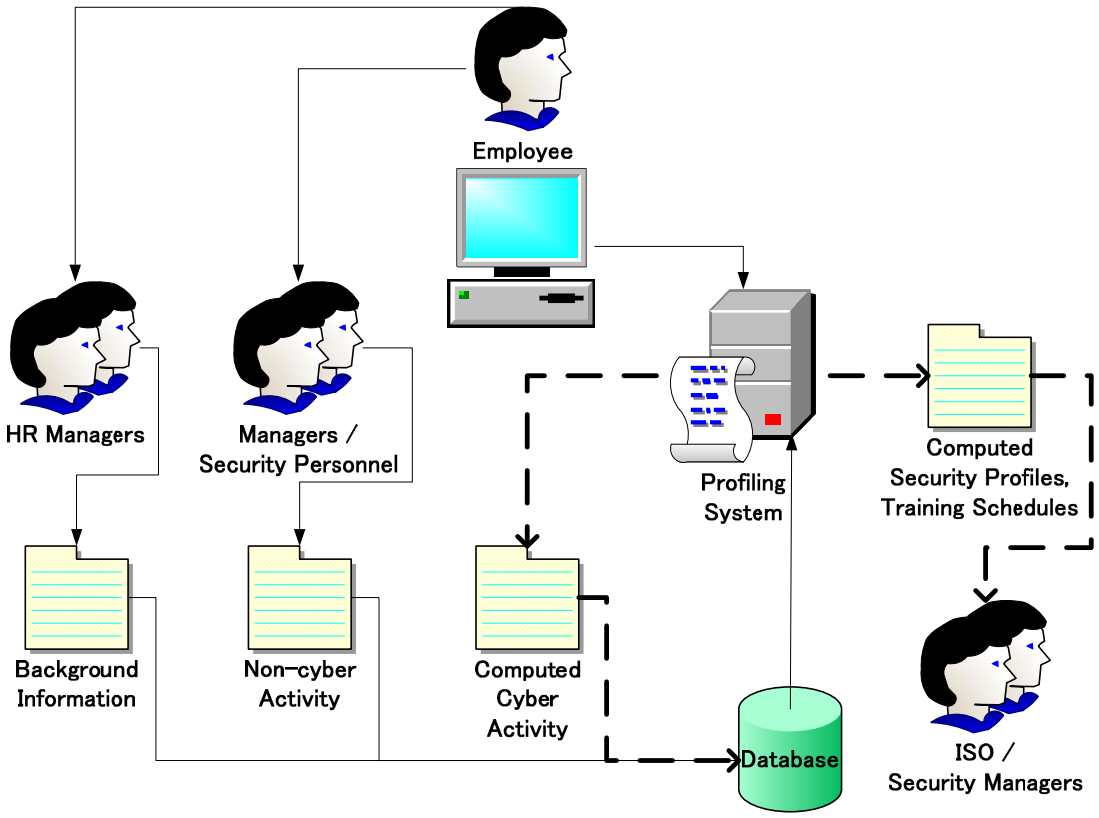

Figure 4.39 – Architecture of the Developed Profiling System

4.3.3.1 Password Security Behaviour

Password Modifying Frequency: The system counts the number of password modifications since joining the organization and during the past 1 year. If the numbers are the same, then the employee might have joined less than a year ago, thus the system checks the number of password modifications in the past 10 months, 8 months and so on until the past month. If the employee joined less than a month ago, it is too new to determine their password modification frequency. If not, the system checks if the password is modified infrequently, few times a year, monthly, every two weeks, weekly, or excessively. If password modification has not been frequent, but has suddenly picked up pace, then it is determined to be a recent activity. Listed in Table 4.1 are the algorithms used for determining password modifying frequency. The functions for 10 months, 8 months, 6 months, 4 months, and 2 months are omitted for brevity. The complete algorithm is listed under Appendix B.

Password Reuse: The system counts the number of total passwords used by the employee in the past 1 year, the number of passwords reused once or twice, the number of passwords reused three-to-five times, the number of passwords reused six-to-nine times, and the number of passwords reused ten times or more in the past year to determine the employee's inclination to reuse passwords. The algorithm for calculating password reuse is listed in Appendix B.

Password Strength: An existing common algorithm, which considers the use of upper- and lower-case letters, numbers and other non-alphanumeric symbols, was reused to check password strength. The algorithm is listed in Appendix B.

Table 4.1 – Algorithm for Determining Password Modifying Frequency

Algorithm

```
Start
    modFreq (modifying frequency), yearly count = count pw changes within last 1 year
    total pw = count all password changes since joining organization
        if (total pw <= yearly count)                                   //joined less than 1 year ago
            ten month count = count pw changes within last 10 months
            if (total pw <= ten month count)                            /joined less than 10 months ago
                eight month count = count pw changes within last 8 months
                ……
                        if (total pw <= monthly count)                  //joined less than 1 month ago
                            modFreq = “Too new to determine”
                        else
                            if(monthly count > 1)
                                modFreq = do 1month
                            else if(monthly count == 1)
                                modFreq = “Monthly”
                            else                                        //monthly count < 1
                                modFreq = “Infrequent”
                ……
            else
                if( ten month count > 3)
                    modFreq = do 10months
                else if(ten month count == 3)
                    modFreq = “Few times yearly”
                else                                                    //ten month count < 3
                    modFreq = “Infrequent”
        else
            if( yearly count > 4)
                modFreq = do 1year
            else if(yearly count == 4)
                modFreq = “Few times yearly”
            else                                                        //yearly count < 4
                modFreq = “Infrequent”
    Return modFreq
Stop
1 year: Start
    modFreq
    yearly count = count pw changes within last 1 year
          if (yearly count <10)
                modFreq = “Few times yearly”
           else                                                         //more than 10 times in the past 1 year
                ten month count = count pw changes within last 10 months
                if (ten month count < yearly count)
                      modFreq = do 10months
                else
                      modFreq = “Recent activity”
    Return modFreq
Stop
1month: Start
    modFreq
    Read monthly count
          If (monthly count < 2)
                modFreq = “Monthly”
          else                                                          //more than once a month
                two week count = count pw changes within last 14 days
                if (two week count < monthly count)
                      modFreq = do 2weeks
```

Algorithm

```
            else
                modFreq = “Recent activity”
    Return modFreq
Stop
Two weeks: Start
    modFreq
    Read two week count
        If (two week count <2)
            modFreq = “Every 2 weeks”
        else                                                    //more than once every 2 weeks
            weekly count = count pw changes within last 7 days
            if (weekly count < two week count)
                if (weekly count < 2)
                    modFreq = “Weekly”
                else                                            //more than once a week
                    modFreq = “Excessively
            else                                        //weekly count is the same as two week count
                modFreq = “Recent activity”
    Return modFreq
Stop
```

4.3.3.2 Data Access & Backup Behaviour

Unauthorized Data Access: The system checks for unauthorized access or attempts to backup data the user is not authorized to access. Data and user security clearance levels are classified into five stages based on their criticality / job titles. For this system implementation, these levels are assumed to be “Public”, “Unclassified”, “Classified”, “Secret”, and “Top Secret” from the lowest to the highest. Since the system uses a “No Read-Up” rule, if an employee attempts to access or backup data of a higher classification than his / her security clearance level, or data for which they have no Need-to-Know, their action is blocked and their profile is updated with the unauthorized access attempt. Access is only granted if data is on the same level or below their clearance level and if they possess the Need-to-Know that information. The algorithms for unauthorized data access and attempted backing up of unauthorized data are listed in Appendix B.

Data Backup Frequency: The system computes the data backup frequency by counting the number of total backups performed by the employee since joining the organization and the number of backups performed in the past month. If these two numbers are the same, then the employee might have joined the organization less than a month ago and it is thus too new to determine their backup frequency. If the employee joined earlier, however, then the system determines if the backup frequency is infrequent, weekly, daily, or excessive. If the employee

used to perform backups at a slower pace, but has recently started backing up more frequently, then the system determines the backup frequency to be a recent activity. The algorithm to compute backup frequency is listed in Appendix B.

4.3.3.3 Behavioural Profiling

The system adapts a rule-based inference system to compile a user security behavioural profile containing the relevant behavioural characteristics for each observable behavioural pattern concerning personally observed non-cyber activities, automatically monitored cyber activities, and background information, by checking the current profile for its characteristics and adding the new characteristics if they are not already listed. The behavioural characteristics shown in Table 4.2 are assumed for each of the following observable behavioural patterns when creating the user security behavioural profiles. The system allows these rules to be configured by the ISO to be aligned with the organization's business objectives. The default values listed in Table 4.2 can serve as general guidelines. "N" depicts not having the corresponding characteristic, while "Y" depicts having that characteristic. The characteristics not relevant to a corresponding observable behaviour are coloured in grey. Thus, according to the default values, the security behavioural profile for an employee who leaves items unattended, for example, will contain the characteristics of not being security conscious, easily revealing information, not valuing or understanding ISM rules, and having a potential for improper sharing of information. The algorithm for compiling security behavioural profiles is listed in Appendix B in summarized form.

Table 4.2 – Behavioural Characteristics for Observable Behavioural Patterns

Activity	Security Conscious	Reveals Information	Values / Understands ISM Rules	Sociable	Ambitious	Technical Knowledge	Easy Hack Target	Suspicious Behaviour	Social Incentive	Career-wise Incentive	Personal Motive	Financial Motive	Psychological Motive	Improper Sharing Potential	Unauthorized Access Potential	Number
Personally Observed Non-Cyber Activities																
Forgets keys	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not forget keys	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Leaves items unattended	N	Y	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not leave items	Y	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Sociable	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	
Not sociable	-	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	
Ambitious	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	Y	
Not ambitious	-	-	-	-	N	-	-	-	-	-	-	-	-	-	-	
Writes down passwords	N	Y	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not write passwords	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Lends keys/PINs	-	Y	-	-	-	-	-	-	Y	-	-	-	-	Y	-	
Does not lend keys/PINs	-	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Security conscious	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Not security conscious	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Understands/values rules	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	
Doesn't understand /value	-	-	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Background Information – Marital Status, Dependents, Academic Record, Financial Status, Criminal Record																
Married									-	-	-	-	-	Y	-	
Unmarried									Y	-	-	-	-	-	-	
Divorced									-	-	Y	-	-	-	-	
Widowed									-	-	-	-	-	-	-	
Dependents												Y				2
BS/MS in Computers						Y									Y	
No BA/BS/MS									Y							
Low income												Y				
Has criminal record													Y		Y	
Cyber Activities – Password Strength																
Very weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Medium	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Strong	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Cyber Activities – Password Modification Frequency																
Infrequent	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Few times a year	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Monthly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Every 2 weeks	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Cyber Activities – Password Reuse																
Ten times or over	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Six-to-nine times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Three-to-five times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	1
Cyber Activities – Attempts to Access Data without Authorization																
Over clearance	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
No need-to-know	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
Cyber Activities – Backup Frequency																
Infrequent	N	-	N	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Daily	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	Y	-	-	Y	-	-	-	-	-	Y	-	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	Y	-	

Asides from the obvious, the reasoning behind this default configuration of security behavioural rules is explained below. Of these, the points concerning marital status are somewhat sensitive topics, thus it is important that these security rules are allowed to be configured to be aligned with the specifications of the organization. For instance, an organization which does not allow the spouse of an employee to be employed at the same organization might hold a firm stance concerning these points, whereas, an organization which is more lenient towards such issues may tend to be more relaxed concerning such points:

- *Low sociability*: leads to social incentives to engage in inappropriate behaviour pertaining to information security (AAAS, 1990), (Lacey, 2009), (Schneier, 2008)
- High ambitiousness: leads to career-wise incentives to engage in inappropriate behaviour pertaining to information security, and potential to access unauthorized information (AAAS, 1990), (Fernando & Asai, 2011_b), (Lacey, 2009)
- Not understanding / valuing ISM rules: leads to potential for improper information sharing (Asai & Fernando, 2011_a), (Asai & Fernando, 2011_b), (Asai, Fernando & Castillo, 2011), (Fernando & Asai, 2011_a), (Fernando & Asai, 2011_b), (Insight Express, 2008), (ISO/IEC 270001, 2005), (Lacey, 2009), (Thapar, 2007)
- Being married: leads to potential for improper information sharing (AAAS, 1990), (Harris & Patten, 2011), (Schneier, 2008)
- Being unmarried: leads to social incentives to engage in inappropriate behaviour pertaining to information security (Harris & Patten, 2011)
- Weak password strength, low password modifying frequency, high reuse of former passwords: leads to potential for improper information sharing (Bishop, 2003), (ISO/IEC 270001, 2005), (Lacey, 2009), (Thapar, 2007)
- Excessive or high recent activity of password modification / data backup: leads to suspicious behaviour (Foley, 2011), (Mills, 2011), (Vroom & von Solms, 2003)

Figure 4.40 displays the number of instances of security behavioural characteristics tested by the default configuration of security rules of this system for each of the observable behavioural patterns.

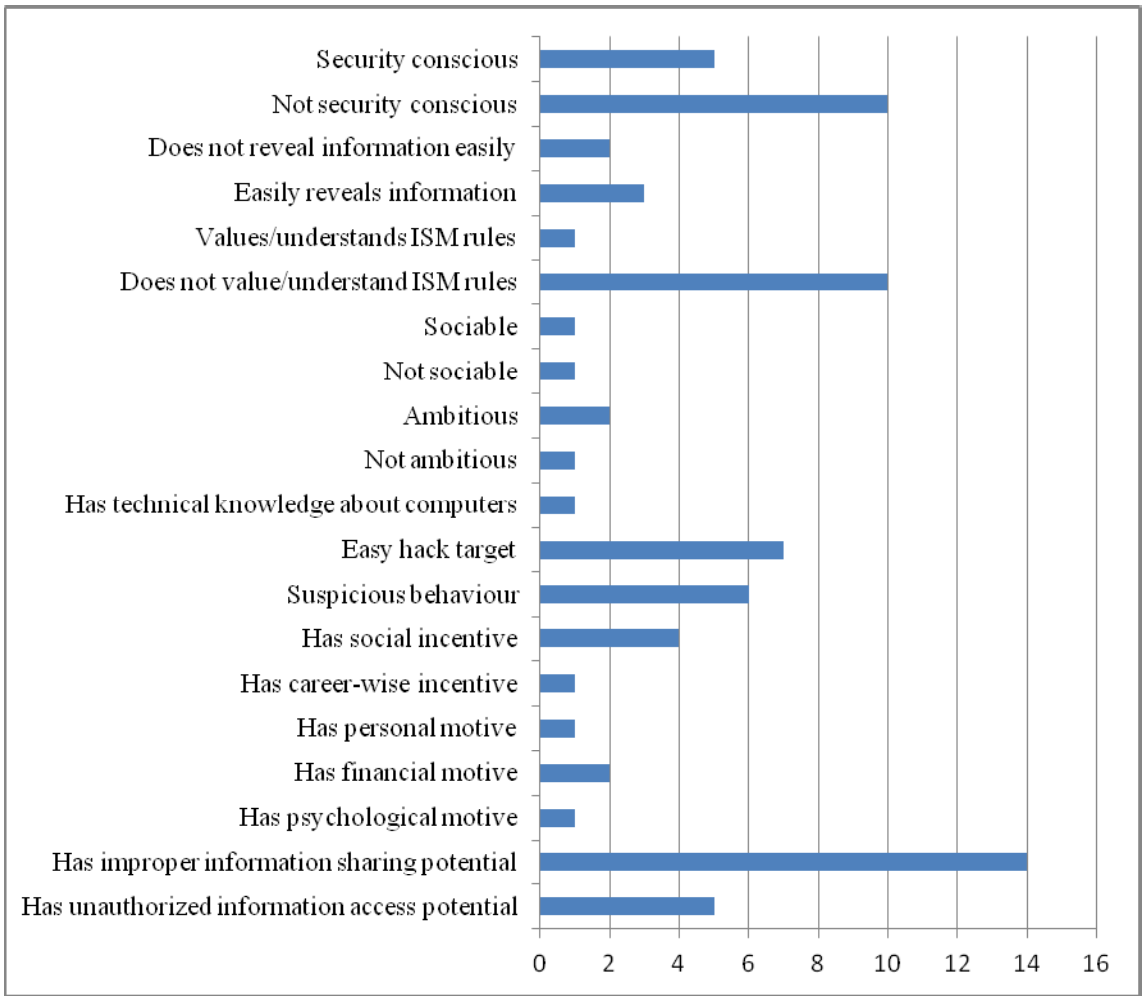

Figure 4.40 – Security Behavioural Characteristics Tested by the Profiling System

As can be seen, corroborating previous researches including (Asai & Fernando, 2011_a), (Asai & Fernando, 2011_b), (Asai, Fernando & Castillo, 2011), (Fernando & Asai, 2011_a), (Fernando & Asai, 2011_b), and (Insight Express, 2008), improper information sharing potential has the highest magnitude, followed by equal magnitudes of not being security conscious, and not valuing or understanding ISM rules, in second place.

4.3.3.4 Scheduling Security Education & Training

The system reads the database to check for any existing security training schedules. If so, the system checks if any of those schedules are yet to come. If there are no available schedules, or if all the available schedules are in the past, then the system re-computes the new schedules. The random schedule for periodic risk perception renewal is set in 4 weeks from

the coming Tuesday for all employees. This will likely consist of a pop-up presentation about security best practices followed by a questioning session to check the employee's understanding of security awareness. For employees who have a potential for improper information sharing, a hands-on security workshop conducted by external security professionals is scheduled in 2 weeks from the coming Wednesday. If an employee has the potential for unauthorized access to information, the system schedules a security seminar by security managers and legal officials in 1 week from the coming Wednesday. For employees who are deemed to have a motive for engaging in improper information sharing or unauthorized access, the system schedules closer inspection and background checks in 2 weeks from the coming Thursday. Thus, the training schedules computed on 30th September 2013 for an employee who requires all four types of security training will include a random awareness training on Tuesday, 29th October 2013, a security workshop on Wednesday, 16th October 2013, a security seminar on Wednesday, 9th October 2013, and a security inspection on Thursday, 17th October 2013. The algorithms for computing security training schedules are listed in Appendix B.

4.4 System Testing

During the system testing phase, each individual component was first checked for accuracy before being integrated together, and subjected to system testing as a whole. In order to conduct these tests, ten hypothetical test case scenarios were created. These hypothetical test cases are described in the subsequent subsection, while the following subsection discusses the test results.

4.4.1 Hypothetical Test Cases

Table 4.3 lists the background information and the job description of the ten hypothetical test cases created to test this system, while table 4.4 lists the hypothetical personal views about the non-cyber activities of these employees observed and inputted by managers and security personnel.

Table 4.3 – Hypothetical Employees

ID	Name	Designation	Marital status	Dependents	Academic Record	Financial Status	Criminal Record
Emp0001	Martha Hall	Accountant	Unmarried	0	BA – Accounting	Steady income	None
Emp0002	Monica White	Software Engineer	Married	1	BS – Computer Science	Steady income	None
Emp0003	Shaun Mills	Computer Operator	Divorced	1	Computer Tech Certification	Low income	Juvenile breaking and entering
Emp0004	John Flynn	Software Engineer	Widowed	2	MS – Computer Engineering	Steady income	Teenaged hacking into Federal Database
Emp0005	Jacob Call	Computer Operator	Married	3	Computer Tech Certification	Low income	None
Emp0006	Faith Stellar	Software Engineer	Divorced	1	MS – Computer Engineering	Steady income	None
Emp0007	Claire McCormick	Accountant	Unmarried	0	BA – Accounting	Steady income	None
Emp0008	Samantha Colt	Computer Operator	Unmarried	1	Computer Tech Certification	Low income	Juvenile shoplifting
Emp0009	Gavin Fields	Accountant	Divorced	3	BA – Accounting	Steady income	None
Emp0010	Sarah Mason	Software Engineer	Married	2	MS – Computer Engineering	Steady income	None

Table 4.4 – Personal Views on Non-Cyber Activity

ID	Manager's View	Security Personnel's View
Emp0001	Forgets keycards	Leaves items unattended
Emp0002	Sociable, ambitious	
Emp0003	Writes down passwords, leaves item unattended	Forgets keycards
Emp0004	Security conscious, ambitious	
Emp0005	Sociable, lends keycards and PINs	Forgets keycards
Emp0006	Security conscious, understands and values ISM rules, ambitious	
Emp0007	Lends keycards and PINs, does not value ISM rules	
Emp0008	Lends keycards and PINs, does not understand or value ISM rules	Lends keycards and PINs, writes down passwords
Emp0009	Ambitious	
Emp0010		

4.4.2 Test Results

The individual components for computing password security behaviour and data backup behaviour were tested for their accuracy of computing cyber activity. Table 4.5 provides an example for computing password modifying frequency for employee Claire McCormick (Emp0007), who joined the organization on 2013/4/2. Password modification frequency is computed on the last date of modifying the password, which is 2013/9/23 for employee Claire McCormick.

Table 4.5 – Password Changes by Employee Claire McCormick (Emp0007)

Password Change ID	**Date**	**Password**	**Strength**
2013-04-02_emp0007_03:40:18	2013-04-02	4cMc7LrI	Medium
2013-04-26_emp0007_03:48:28	2013-04-26	LcM7cC01	Medium
2012-05-31_emp0007_21:24:16	2012-05-31	RaI007lC	Medium
2013-06-28_emp0007_21:16:28	2013-06-28	LcM7cC01	Medium
2013-07-19_emp0007_21:24:43	2013-07-19	cL7MM92c	Medium
2013-08-22_emp0007_19:25:26	2013-08-22	LcM7cC01	Medium
2013-09-23_emp0007_01:41:07	2013-09-23	cCmC7k05	Medium

Table 4.6 shows the resulting password security behaviour for Claire McCormick, which shows that she modifies her password “Monthly” and that out of a total of 7 passwords used, she had reused no passwords ten times or more, 0 passwords were reused six-to-nine times, 1 password was reused three-to-five times and 4 passwords were used once or twice.

Table 4.6 – Password Security Behaviour of Claire McCormick (Emp0007)

Employee ID	**Password Strength**	**Reuse**	**Password Modifying Frequency**
Emp0007	Medium	7_0_0_1_4	Monthly

Table 4.7 provides an example for computing backup frequency for employee Gavin Fields (Emp0009), who joined the organization on 2009/10/1. The data backing up of the last 6 months by Gavin Fields is displayed. Backup frequency is computed on the last date of performing data backup, which is 2013/9/30 for employee Gavin Fields. Table 4.8 shows that

the resulting backup behaviour for Gavin Fields shows that his performing of data backup is computed to be of “Recent activity”, since he has been modifying it monthly up until 2013/8/23, and since then, his backing up of data has picked up pace and he has been performing data backups more frequently; sometimes even multiple times a day.

Table 4.7 – Data Backup by Employee Gavin Fields (Emp0009)

Data Backup ID	Employee ID	Date
2013-03-22_emp0009_20:18:23	Emp0009	2013-03-22
2013-04-26_emp0009_21:55:46	Emp0009	2013-04-26
2013-05-24_emp0009_21:58:47	Emp0009	2013-05-24
2013-06-28_emp0009_19:55:30	Emp0009	2013-06-28
2013-07-22_emp0009_21:55:53	Emp0009	2013-07-22
2013-08-23_emp0009_21:55:34	Emp0009	2013-08-23
2013-09-06_emp0009_21:55:56	Emp0009	2013-09-06
2013-09-06_emp0009_21:55:57	Emp0009	2013-09-06
2013-09-09_emp0009_17:36:48	Emp0009	2013-09-09
2013-09-13_emp0009_21:55:59	Emp0009	2013-09-13
2013-09-22_emp0009_20:56:01	Emp0009	2013-09-22
2013-09-22_emp0009_20:56:02	Emp0009	2013-09-22
2013-09-22_emp0009_21:56:03	Emp0009	2013-09-22
2013-09-22_emp0009_22:02:56	Emp0009	2013-09-22
2013-09-30_emp0009_13:06:20	Emp0009	2013-09-30
2013-09-30_emp0009_13:06:22	Emp0009	2013-09-30
2013-09-30_emp0009_14:05:25	Emp0009	2013-09-30
2013-09-30_emp0009_14:05:30	Emp0009	2013-09-30
2013-09-30_emp0009_16:08:34	Emp0009	2013-09-30
2013-09-30_emp0009_16:53:09	Emp0009	2013-09-30

Table 4.8 – Backup Behaviour of Gavin Fields (Emp0009)

Employee ID	Backup Frequency
Emp0009	Recent activity

The results of these tests prove the accuracy of computing cyber activity by this implemented system. Table 4.9 shows the automatically monitored and computed cyber activity for all ten of these hypothetical employees.

Table 4.9 – Computed Cyber Activity

ID	Password Strength	Password Reuse	Password Modifying Frequency	Backup Frequency	Access Over Clearance	Access Without Need-to-Know
Emp0001	Medium	19_0_1_2_3	Every 2 weeks	Daily	0	0
Emp0002	Medium	12_0_0_2_5	Weekly	Excessive	0	2
Emp0003	Weak	20_0_1_2_2	Excessive	Excessive	2	1
Emp0004	Strong	13_0_0_0_12	Every 2 weeks	Weekly	0	0
Emp0005	Medium	3_0_0_0_3	Few times yearly	Infrequent	1	0
Emp0006	Strong	8_0_0_0_8	Monthly	Daily	0	0
Emp0007	Medium	7_0_0_1_4	Monthly	Weekly	0	0
Emp0008	Weak	2_0_0_0_2	Infrequent	Infrequent	5	5
Emp0009	Medium	18_0_0_3_2	Recent activity	Recent activity	2	3
Emp0010	Strong	3_0_0_0_3	Too new to determine	Too new to determine	0	1

Table 4.10 depicts the MBTI personality types and resulting personalities of the employees as deemed true by the system according to the monitored cyber and non-cyber activities, and background information. The resulting personalities for each of the personality types listed in table 4.10 are adapted from the Myers & Briggs Foundation. A "?" mark is used to depict an indeterminable dichotomy of personal preference, in which case the personality type and personality cannot be determined completely.

Table 4.10 – Computed Personality Types and Personalities.

ID	Personality Type	Personality
Emp0001	?SF?	Cannot determine personality
Emp0002	IN?P	Cannot determine personality
Emp0003	ISFP	Friendly, sensitive, likes own space and own time, loyal, committed, dislikes conflicts, enjoys present moment.
Emp0004	INTP	Seeks explanations, theoretical, not sociable, focused, analytical.
Emp0005	ESFP	Outgoing, friendly, accepting, loves material comforts, sociable, realistic, spontaneous.
Emp0006	INTJ	Develops perspectives, achieves goals, skeptical, has high performance standards.
Emp0007	ESFP	Outgoing, friendly, accepting, loves material comforts, sociable, realistic, spontaneous.
Emp0008	?SFP	Cannot determine personality
Emp0009	I??P	Cannot determine personality
Emp0010	INTP	Seeks explanations, theoretical, not sociable, focused, analytical.

Table 4.11 depicts the results obtained from the security behavioural profiling system on 2013/9/30. By comparing the data in table 4.10, concerning the personalities of the employees, with the resulting behavioural profiles in table 4.11, it can be seen that MBTI personality types and their resulting personalities match the behavioural profiles with sufficient accuracy. Thus, it is safe to assume that in the case the MBTI personality types of the employees of an organization are determined they could be used to provide insight into the behavioural patterns of the employees to a certain extent.

These resulting profiles and security education and training schedules seen in table 4.11 show that employees, Monica White (Emp0002), Shaun Mills (Emp0003), Jacob Call (Emp0005), Samantha Colt (Emp0008) and Gavin Fields (Emp0009) have security behavioural flaws that could lead to information security problems along with motives or incentives, and thus need the hands-on training workshop, security educational seminar and closer inspection, along with the random security awareness. Employee Martha Hall (Emp0001), on the other hand requires the hands-on training workshop and closer inspection, along with the random security awareness program. Employees John Flynn (Emp0004) and Faith Stellar (Emp0006) do not engage in any wrongful security behaviour, but their knowledge about computers and their background information show that they still require the security seminar showing the legal aspects of security violations, along with closer inspection and the random security awareness. Employee Sarah Mason (Emp0009) is too new for the system to identify her security traits yet, but since she has already tried to access data without need-to-know once, and due to her background information, she requires the hands-on training workshop and security seminar, along with the random security awareness. Employee Claire McCormick (Emp0007), however, is an example of a case where the personal views of her manager might be biased. Her cyber activities and background information show that she does not engage in any wrongful security behaviour, but the personal views state otherwise. In this instance, the ISO can request for separate views of her security profile, and upon seeing that the personal observations by her manager contradict the rest of her security traits determined by the system, can use his or her own personal judgement to avoid any personal bias this employee's manager might have towards her, and thereby decide whether she requires the hands-on training workshop, or whether closer inspection and the random security awareness program are sufficient.

Table 4.11 – Computed Security Behavioural Profiles, Security Status, and Security Education and Training Schedules

ID	Profile	Security Status	Random Schedule	Workshop Schedule	Seminar Schedule	Inspection Schedule
Emp0001	Not security conscious. Information revealed easily. Does not understand or value ISM rules. May have social incentives. Easy hack target.	Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	None	2013_10_17
Emp0002	Sociable. Ambitious. May have career-wise incentives. Has technical knowledge about computers. Not security conscious. Does not understand or value ISM rules. Easy hack target. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0003	Not security conscious. Information revealed easily. Does not understand or value ISM rules. May have personal motives. May have social incentives. May have financial motives. May have psychological motives and potential. Suspicious behaviour. Easy hack target. Ambitious.	Has unauthorized access potential. Has improper sharing potential. Has motives / incentives	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0004	Ambitious. May have career-wise incentives. Security conscious. Has technical knowledge about computers. May have psychological motives and potential.	Has unauthorized access potential. Has motives / incentives.	2013_10_29	None	2013_10_9	2013_10_17
Emp0005	Sociable. Information revealed easily. May have social incentives. Not security conscious. May have financial motives. Does not understand or value ISM rules. Easy hack target. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0006	Ambitious. May have career-wise incentives. Security conscious. Understands and values ISM rules. May have personal motives. Has technical knowledge about computers.	Has unauthorized access potential. Has motives / incentives.	2013_10_29	None	2013_10_9	2013_10_17
Emp0007	Information revealed easily. May have social incentives. Does not understand or value ISM rules.	Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	None	2013_10_17
Emp0008	Information revealed easily. May have social incentives. Does not understand or value ISM rules. Not security conscious. May have financial motives. May have psychological motives and potential. Easy hack target. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0009	Ambitious. May have career-wise incentives. May have personal motives. May have financial motives. Suspicious behaviour. Not security conscious. Does not understand or value ISM rules. Easy hack target.	Has unauthorized access potential. Has improper sharing potential. Has motives / incentives.	2013_10_29	2013_10_16	2013_10_9	2013_10_17
Emp0010	Has technical knowledge about computers. Security conscious. Does not understand or value ISM rules. Suspicious behaviour.	Has unauthorized access potential. Has improper sharing potential.	2013_10_29	2013_10_16	2013_10_9	None

These results prove that the anticipated outcomes of the hypothetical test cases were satisfactorily reflected through the security behavioural profiles compiled by this system. In order to ensure the accuracy of profiling security behaviour based on non-cyber activity and background information, the next section uses some real-life test case scenarios obtained from other researches (Okayasu, 2014) for profiling.

4.4.3 Real-Life Test Cases & Test Results

Table 4.12 – Real-Life Test Case Scenarios

Case	Background Information	Non-cyber Activity	Profile	Outcome
Case A	IT genius, many academic accolades from MIT and Stanford. College dropout.	Did not understand ISM rules (cybercrime, fraud, copyright violations).	Has technical knowledge. May have social incentives. Does not understand or value ISM rules. Improper sharing potential.	Hacked into digital library and released academic journals for free.
Case B	Computer geek. Not sociable. Has gender identity disorder. Lowest rank in US military.	Accessed information over clearance (during transportation). Does not understand or value ISM rules.	Has technical knowledge. Not sociable. May have social incentives. Does not understand or value ISM rules. Has improper sharing potential. Has unauthorized access potential. Suspicious behavior.	Released secret diplomatic and military documents to Wikileaks.
Case C	Gifted programmer and shrewd journalist. Won accolades for whistle-blowing. Criminal record for hacking and rape and on Interpol criminal list. Divorced.	Does not value ISM rules → makes his own rules and justifications.	Has technical knowledge. May have psychological motive and potential. May have social incentives. Does not understand or value ISM rules. Has improper sharing potential. Has unauthorized access potential. May have personal motives.	Founded Wikileaks.
Case D	Computer geek. High school dropout (General Education Development Diploma). 2-year community college-graduate. Discharged from military due to injury. Security personnel at NSA. IT operative at CIA.		Has technical knowledge. May have social incentives.	Collected and copied secret surveillance dossier (without need-to-know) and released the information.

**Note: The background information, non-cyber activity, and outcomes of these real-life test cases were obtained from Okayasu (2014).*

Example real-life test cases, the security behavioural profiles compiled by the system for these test cases, and the outcomes that occurred in these scenarios are listed in Table 4.12. The resulting security behavioural profiles of these real-life test case scenarios prove the accuracy of profiling, using non-cyber activity and background information, by this system.

4.5 Engineering Challenges

The main engineering challenge faced by this research was during its evaluation phase, where it was not possible to evaluate the system for accuracy of computing cyber activity using real test data from real system users. Since the system requires gathering information about users' behaviour over a period of time it cannot be evaluated using real test data unless it was deployed for beta-testing on a business organization with sufficient information assets.

The system was, however, tested for the accuracy of computing cyber activity, and for the accuracy of compiling security behavioural profiles based on computed cyber activity, non-cyber activity, and background information of hypothetical test cases. In addition, the system implementation was also tested for the accuracy of compiling security behavioural profiles based on non-cyber activity and background information of real-life test cases. Further, the system was also evaluated for its usability and performance by real users during the evaluation phase of the research. The usability evaluation of this system is discussed in detail in the next chapter.

4.6 Discussion

The system presented through this research addresses the problem of improper sharing of information by insiders with outsiders or unauthorized insiders, and provides a workable solution to achieve internal control of information sharing within an organization. By examining the automatically monitored cyber activities of the employees, their non-cyber activities personally observed by their managers or security personnel of the organization, and their background information, the system compiles security behavioural profiles showing which of the employees could potentially engage in which wrongful activities that could present a threat to the organization's information security. Accordingly, the system also

determines and schedules the level and type of security education and training to be given to each individual employee.

By allowing observable information about employees' non-cyber behaviour to be inputted personally by managers and security personnel, and through automatic monitoring of cyber-activities of employees, this system attempts to handle the human-related problem of improper information sharing using both technological and social information gathering methods. It also provides a solution containing a socio-technological system employing automatic access control, logging, and risk perception renewals by the system, along with hands on security awareness and training workshops conducted by security professionals, and the allowing of the use of personal judgement by the ISO. By providing a mix of social and technological methods and techniques, the system enables an organization to provide a workable managerial solution to this human-related problem of information security and thereby overcomes the weaknesses of a purely technological solution.

Monitoring of employees' activities does, however, produce privacy implications. This system keeps such implications to a minimal by providing the two separate "strict" and "relaxed" modes to clearly distinguish the times when monitoring of activities will or will not be conducted.

By allowing the ISO to configure the security behavioural rules to be aligned with the business objectives of the organization, this system can be tailor-made to suit the specific requirements of the organization. Further, the summarized, detailed, graphical and separate views of security behavioural profiles and the graphical display of security education and training schedules provide convenience to the ISO and security managers.

The modules concerning the monitoring of employees' password security behaviour, data access and backup behaviour, personal observations of employee behaviour, gathering information obtained through background checks, configuration of security behavioural rules, compilation of user security behavioural profiles and scheduling of security education and training were developed during the system implementation phase using a rule-based inference method.

Through the results obtained by testing the system presented above with the hypothetical test cases, it can be stated that this system can accurately compute employee cyber activity. Further, through the results obtained by testing the system implementation on both hypothetic and real-life test cases, it can be stated that the system can be used for accurately profiling and effectively predicting potential security infractions and information security behavioural flaws by employees within an organization to a certain extent.

The next chapter discusses the usability evaluation of this system.

Chapter 5

System Usability Evaluation

Chapter 5

System Usability Evaluation

5.1 Introduction

The system was evaluated for its usability and performance, and the evaluation process and its results are discussed in this chapter.

The ten hypothetical test case scenarios used for the testing of this system and explained in section 4.4 were also used for the usability evaluation of this system. The usability evaluation of this system was carried out as explained below:

The respondent pool of 24 was divided into three separate groups with 8 respondents each: group A, group B, and group C. The respondents of all groups were asked to assume they were the ISO of a business organization and to compile security behavioural profiles and security education and training schedules based on the information gathered by the security behavioural profiling system about the ten hypothetical employees as of 2013 September 30th. Group A was given tabular data for each employee, instructions for computing cyber activity, compiling security behavioural profiles, and for determining and scheduling security education and training programmes. Group B was requested to use the developed system to obtain textual results compiled by the system. Group B was further given instructions for determining and scheduling security education and training programmes. Group C was requested to use the developed system to obtain graphical results compiled by the system. The data, instructions, and systems given to each of these three groups are summarized in table 5.1. The instructions given to each of these groups and the evaluation survey questionnaires, along with the tabular data provided to Group A, are listed under Appendix C.

Table 5.1 – Usability Evaluation Groups

Group A	**Group B**	**Group C**
Tabular data of employees' cyber activity	Use implemented profiling system	Use implemented profiling system
Instructions to manually compute cyber activity: password modifying frequency, password reuse, data backup frequency, etc.	View textual results: compiled profiles in summarized form, in detailed form, and in separate form (where behavioural characteristics pertaining to cyber activities, non-cyber activities, and background information, are viewed separately)	View graphical results: compiled profiles in graphical form, computed security education and training schedules displayed graphically on a calendar
Instructions and rules to manually compile security behavioural profiles		
Instructions to manually compute security education and training schedules	Instructions to manually compute security education and training schedules	

Figure 5.1 depicts the summarized profile for employee Samantha Colt (Emp0008), while figures 5.2, 5.3, 5.4, and 5.5 display the detailed profile, separate views, graphical profile, and the graphical display of security education and training schedules on a calendar for the same employee. The GUIs depicting the summarized, detailed, and graphical profiles, as well as the profiles as separate views, along with the security education and training schedules, for the rest of the hypothetical employees are listed under Appendix A.

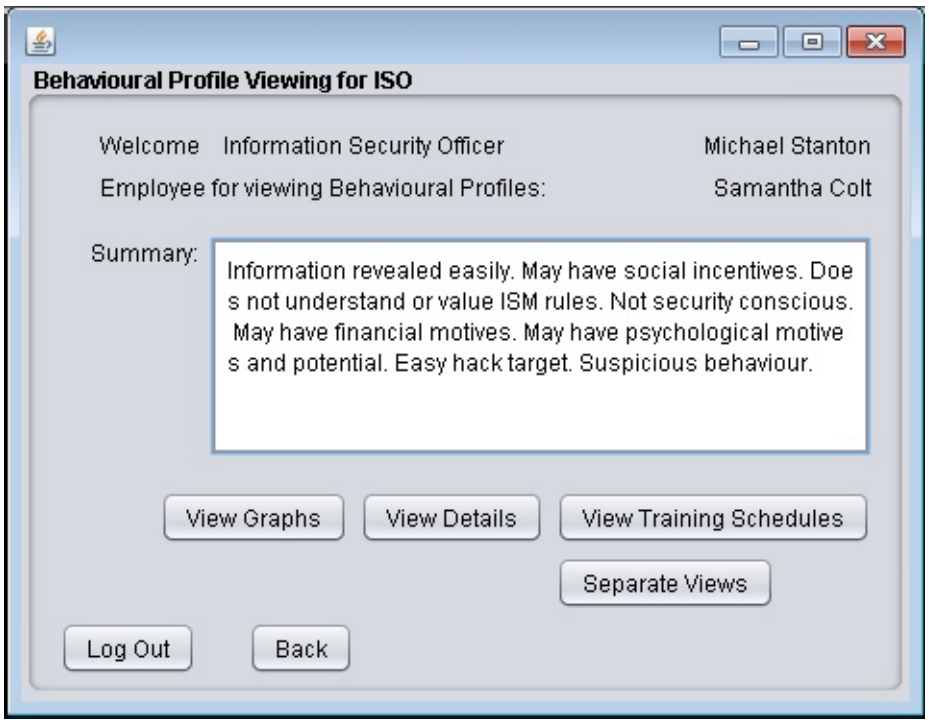

Figure 5.1 – Summarized Behavioural Profile of Samantha Colt (Emp0008)

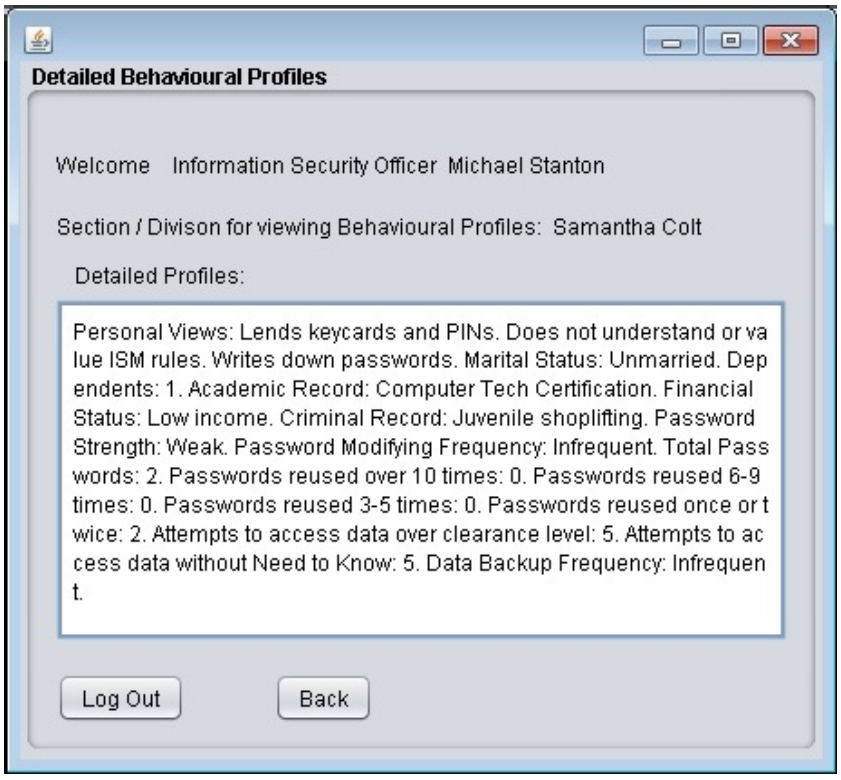

Figure 5.2 – Detailed Behavioural Profile of Samantha Colt (Emp0008)

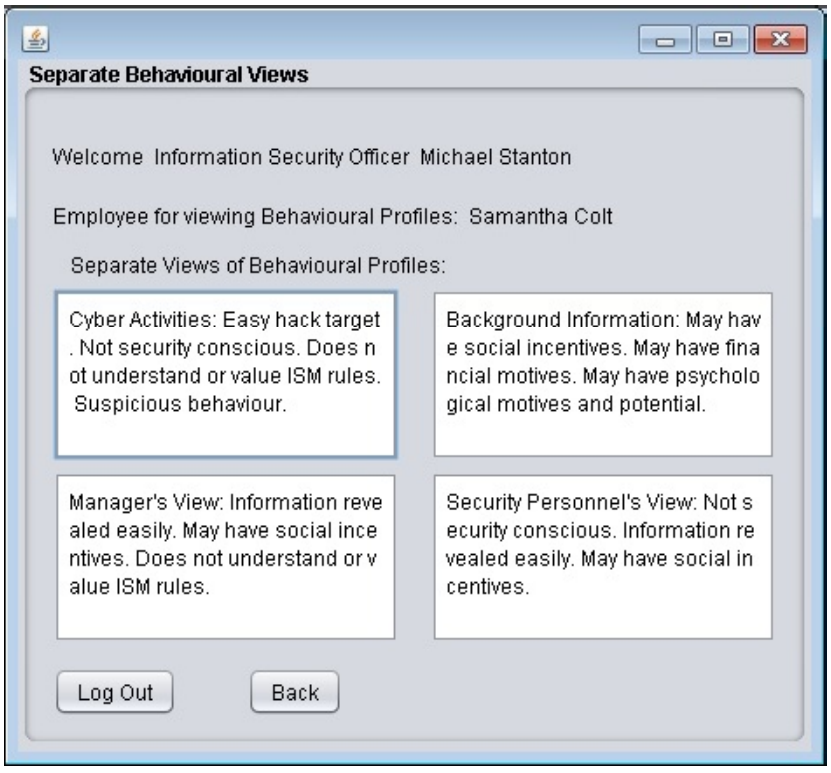

Figure 5.3 – Separate Views of the Behavioural Profile of Samantha Colt (Emp0008)

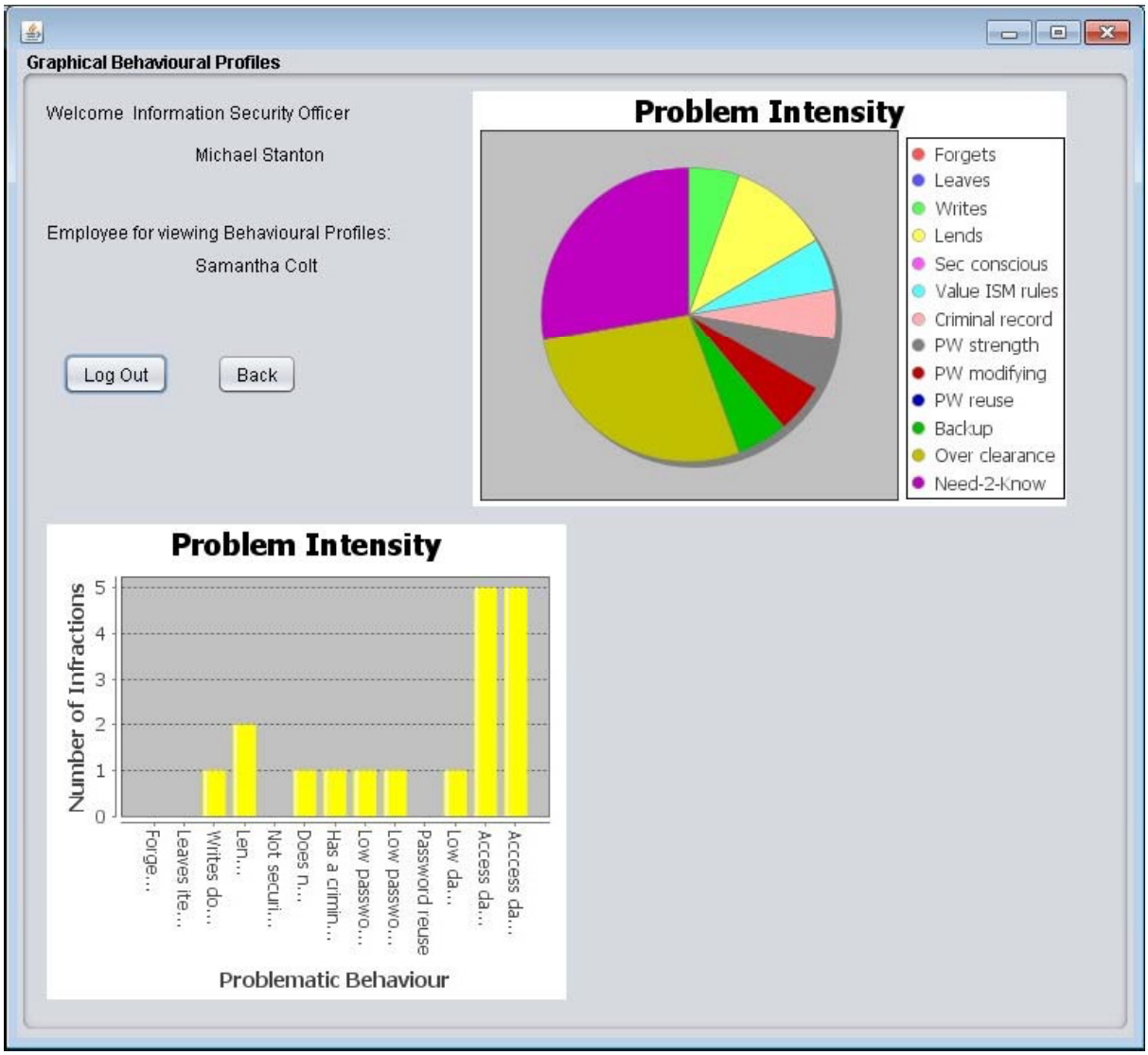

Figure 5.4 – Graphical Behavioural Profile of Samantha Colt (Emp0008)

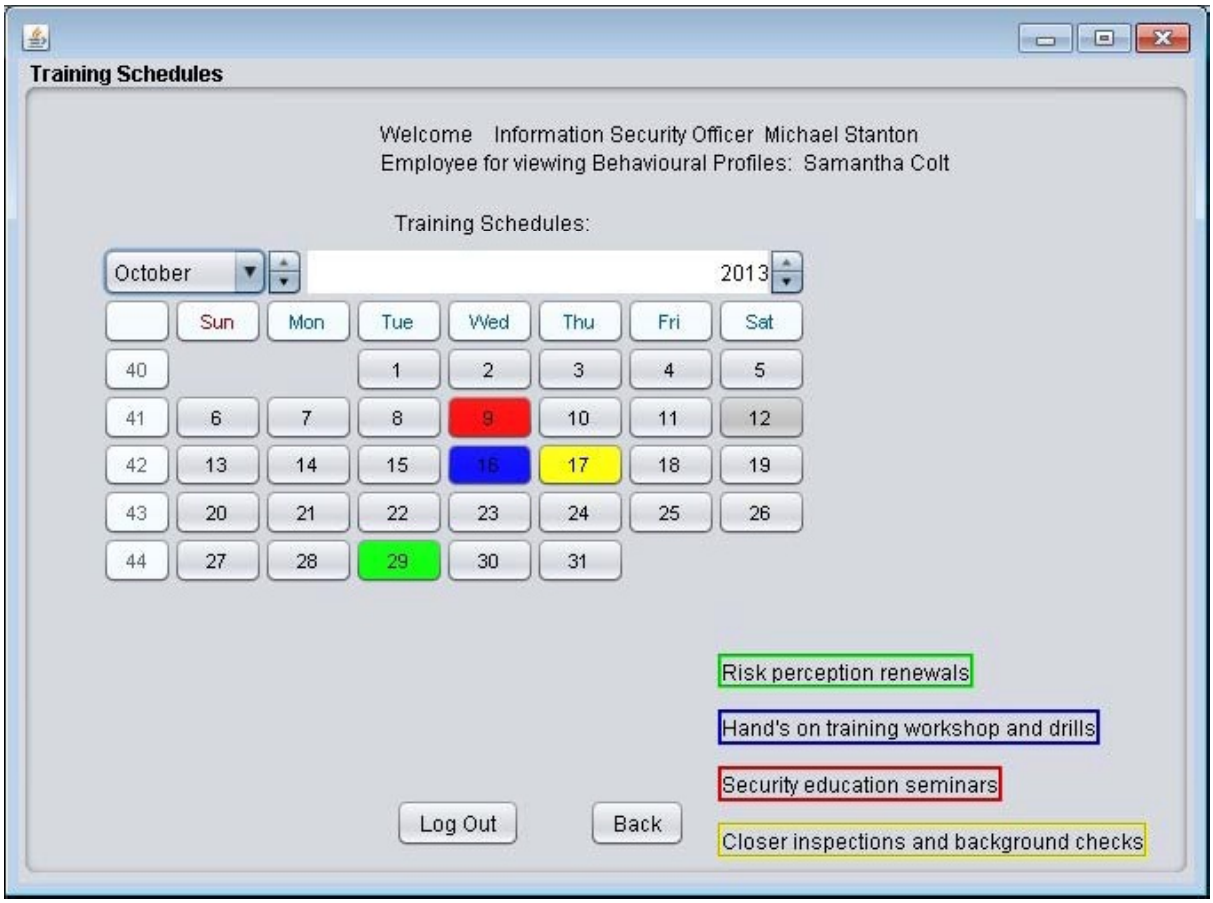

Figure 5.5 – Security Education and Training Schedules for Samantha Colt (Emp0008)

The following aspects were evaluated:

- Speed of arriving at decisions concerning security behaviour
- Speed of scheduling security education and training
- Amount of computations needed for determining security behaviour
- Amount of computations needed for scheduling security education and training
- Presentation
- Amount of detail
- Usefulness of presented data
- Ease of determining potential or motive for improper information sharing or unauthorized data access
- Ease of recognizing personal bias
- Overall usability

The respondents were asked to rate each of these evaluation aspects on a scale of one to five ranging from “Very poor” through “Very good”.

5.2 Respondent Characteristics

The respondents consisted of well-versed computer users of many nationalities and from many different occupations. The characteristics of the respondents belonging to each group and as a whole are depicted in tables 5.2 through 5.5.

Table 5.2 – Respondent Characteristics of Group A

Group A:		Tabular data	8
Nationality		**Occupation**	
Sri Lankan	3	Graduate student	1
American	1	Undergraduate	1
Mexican	1	Professor	1
Japanese	2	Teacher	1
British	1	Software Architect	1
Residing country		Secretary	1
Japan	3	Office worker	1
Sri Lanka	3	Doctor	1
United States	1		
United Kingdom	1		

Table 5.3 – Respondent Characteristics of Group B

Group B:		Textual profiles	8
Nationality		**Residing country**	
Sri Lankan	4	Japan	8
Japanese	2	**Occupation**	
Venezuelan	1	Graduate student	8
Nepalese	1		

Table 5.4 – Respondent Characteristics of Group C

Group C:		Graphical profiles	8
Nationality		**Residing country**	
Sri Lankan	2	Japan	8
Japanese	3	**Occupation**	
Mongolian	1	Graduate student	6
Chinese	1	Undergraduate	2
Indian	1		

Table 5.5 – Combined Respondent Characteristics

Total	24	**Residing country**	
		Japan	19
Nationality		Sri Lanka	3
Sri Lankan	9	United States	1
American	1	United Kingdom	1
Mexican	1	**Occupation**	
Japanese	7	Graduate student	15
British	1	Undergraduate	3
Venezuelan	1	Professor	1
Nepalese	1	Teacher	1
Mongolian	1	Software Architect	1
Chinese	1	Secretary	1
Indian	1	Office worker	1
		Doctor	1

5.3 Evaluation Results

The results of the system usability evaluation are presented in this section. The subsequent subsections examine the evaluation results of each of these separate groups, as well as the overall comparison of results across these three groups. Figure 5.6 depicts the evaluation

results for group A, while the evaluation results for groups B and C are depicted in figures 5.7 and 5.8, respectively.

5.3.1 Group A – Tabular Data

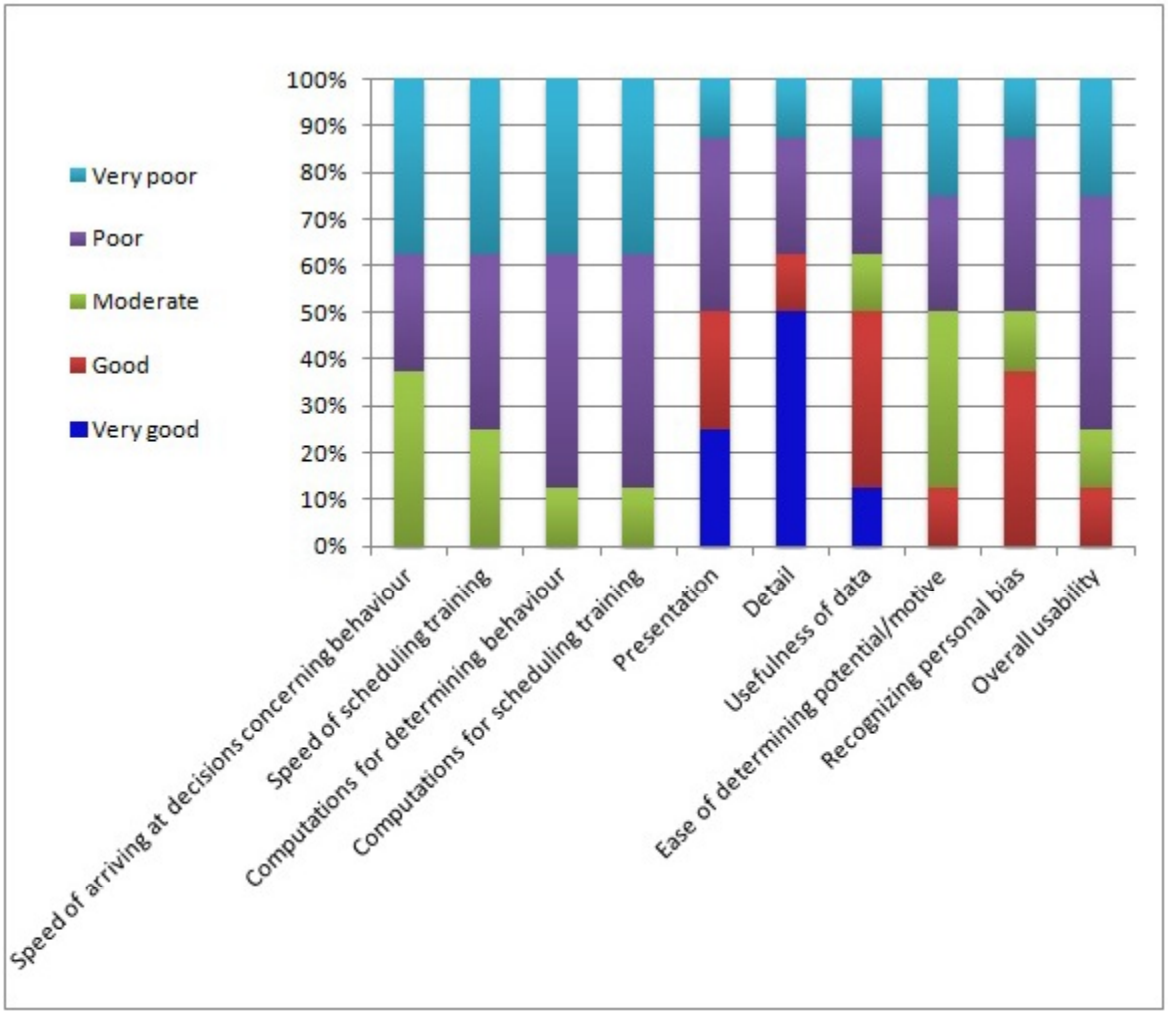

Figure 5.6 – Evaluation Results for Group A – Using Tabular Data for Manually Computing Behavioural Profiles and Security Education and Training Schedules

As can be seen through these evaluation results, the speed of arriving at decisions concerning security behaviour and the speed of scheduling security education and training for group A ranged from “Very slow” through “Moderate”, while the amount of computations for determining behaviour and for scheduling security education and training ranged from “Extensive” through “Moderate”. The presentation, amount of detail, and usefulness of data for group A spanned the entire range from “Very low” to “Very high”, while the ease of

determining potential or motive, recognizing personal bias, and overall usability of the system ranged from “Very low” through “High”.

5.3.2 Group B – Textual Results

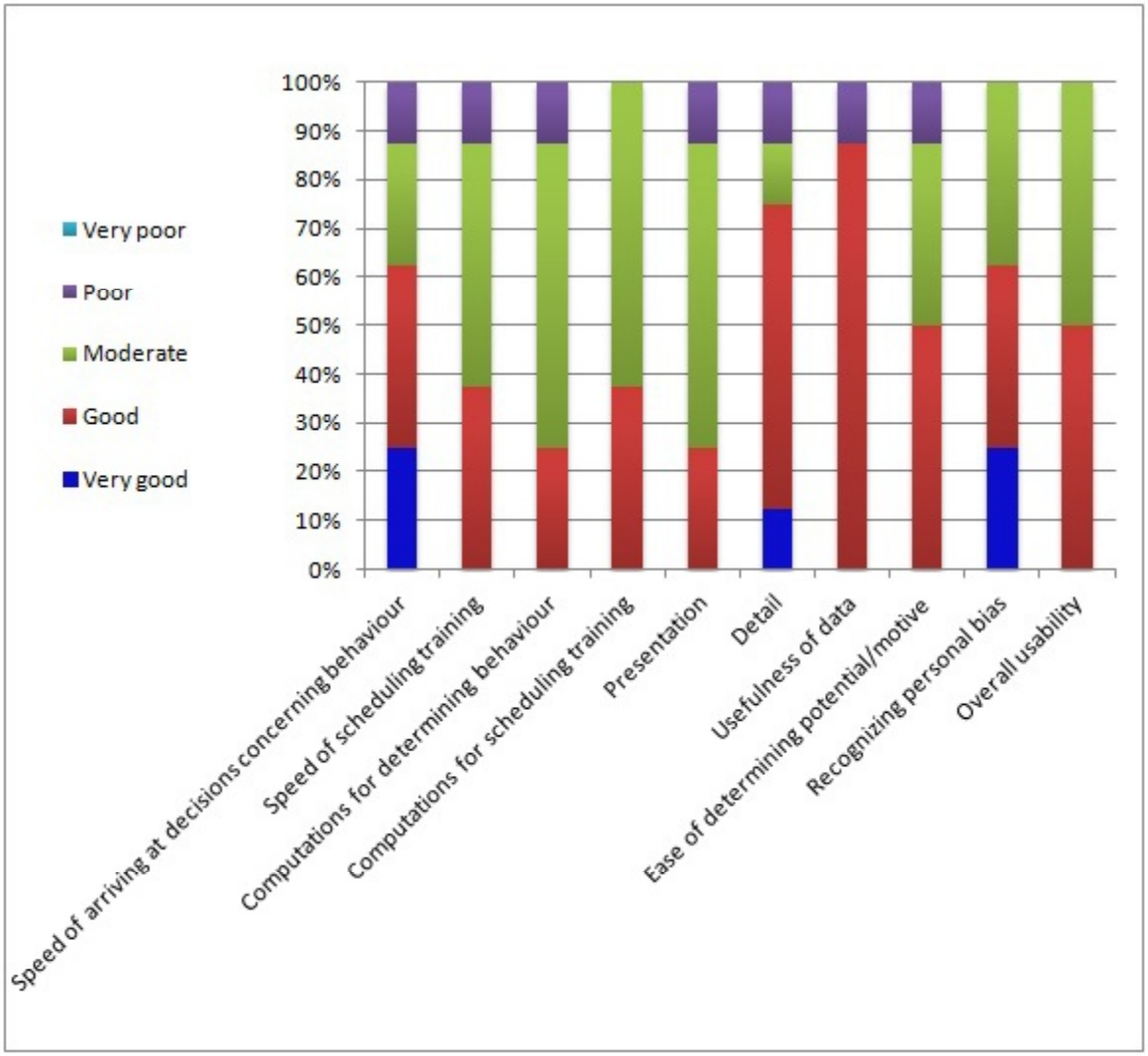

Figure 5.7 – Evaluation Results for Group B – Using Textual Profiles Compiled by the Profiling System, and Manually Computing Security Education and Training Schedules

The speed of arriving at decisions concerning behaviour ranged from “Slow” to “Very fast” for group B, while the speed of scheduling security education and training ranged only from “Slow” to “Fast”. This difference in speeds of arriving at decisions concerning behaviour and scheduling security education and training, is explained by the fact that group B had to

compute the security education and training schedules manually. The amount of computation needed by group B and the presentation of information to group B were mostly evaluated as being “Moderate”, while the amount of detail, usefulness of data, and the ease of determining potential or motive were deemed to be mostly “High”. The ease of recognizing personal bias ranged from “Moderate” to “Very high” for group B, while the overall usability of the system presented to group B was equally divided between “Moderate” and “High”.

5.3.3 Group C – Graphical Results

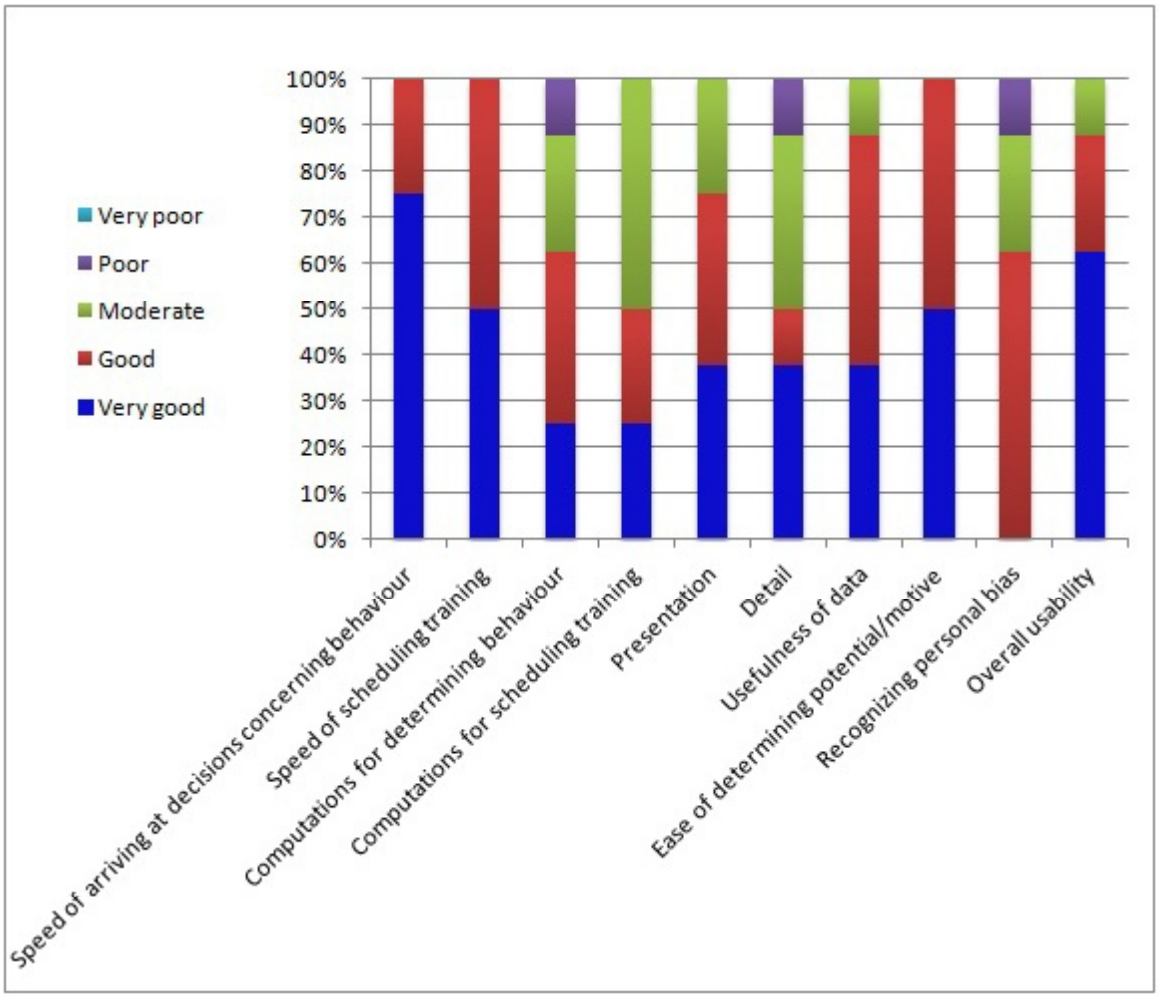

Figure 5.8 – Evaluation Results for Group C – Using Graphical Profiles and Security Education and Training Schedules Compiled by the Profiling System

For group C, the speeds of arriving at decisions concerning behaviour and scheduling education and training were either “Fast” or “Very fast”, while the amount of computations

for determining behaviour ranged from “Large” to “Very small”, and the amount of computations for scheduling education and training ranged from “Moderate” to “Very small”. The presentation of the system, and the usefulness of the data, ranged from “Moderate” through “Very high” for group C. The amount of detail ranged from “Low” through “Very high”, while the ease of determining potential or motive was equally divided between “High” and “Very high”. The ease of recognizing bias, however, ranged only from “Low” to “High”. The overall usability of the system is deemed mostly as “Very high” for group C.

Through these graphs it can be seen that there is a drift from “Very poor” to “Very good” from group A through C. To further explore this drift, the next subsection compares the results across these three groups.

5.3.4 Overall Evaluation Results – Comparison across Groups

Figures 5.9 through 5.18 depict the comparison of evaluation results across the three groups for each of the ten aspects of evaluation.

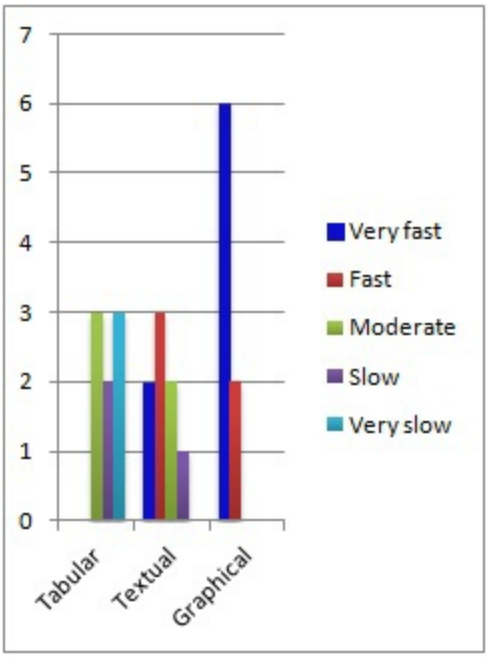

Figure 5.9 – Comparison of Results for Speed of Arriving at Decisions concerning Security Behaviour

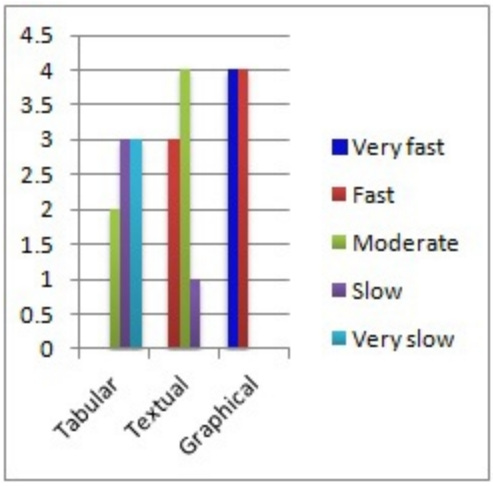

Figure 5.10 – Comparison of Results for Speed of Scheduling Security Education and Training

From figure 5.9 it can be seen that the speed of arriving at decisions concerning security behaviour is moderate, slow or very slow when using tabular data, whereas it is mostly moderate, fast or very fast when using textual results, and mostly very fast when using graphical results. Figure 5.10 shows that the speed of scheduling security education and training is very slow through moderate when using tabular data, mostly moderate or fast when using textual results, and either fast or very fast when using graphical results.

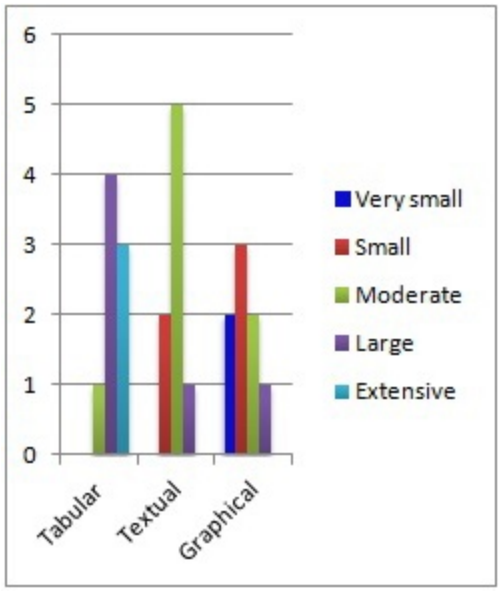

Figure 5.11 – Comparison of Results for Amount of Computations for Determining Behaviour

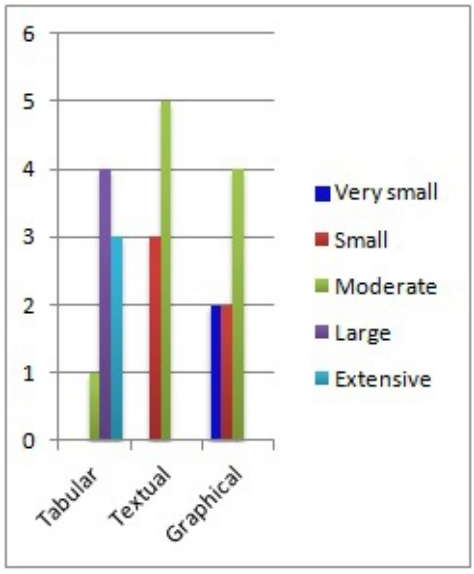

Figure 5.12 – Comparison of Results for Amount of Computations for Scheduling Security Education and Training

Figures 5.11 and 5.12 depict that the amounts of computations for determining behaviour and for scheduling security education and training are mostly large or extensive when using tabular data, whereas, they are mostly moderate when using textual results. When using graphical results, the amount of computations for determining behaviour range from very small through large, and the amount of computations for scheduling security education and training range from very small through moderate.

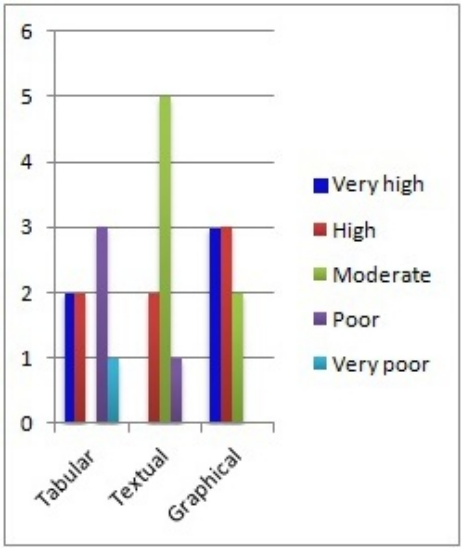

Figure 5.13 – Comparison of Results for Presentation

The presentation of data is mostly poor when using tabular data, mostly moderate when using textual results and is mostly high or very high when using graphical results.

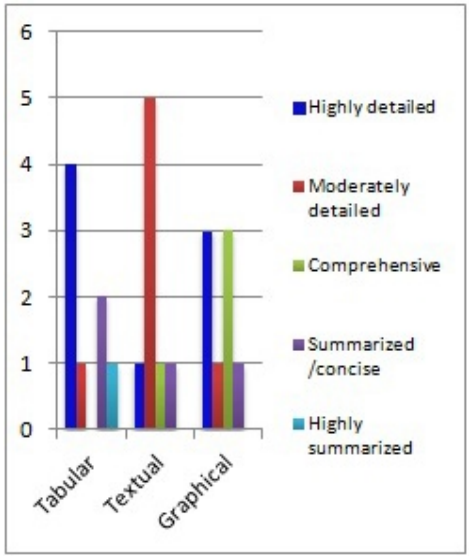

Figure 5.14 – Comparison of Results for Amount of Detail

The amount of detail gleaned from tabular data is mostly high, while textual results provide mostly moderately detailed information, and graphical results provide mostly comprehensive or highly detailed information.

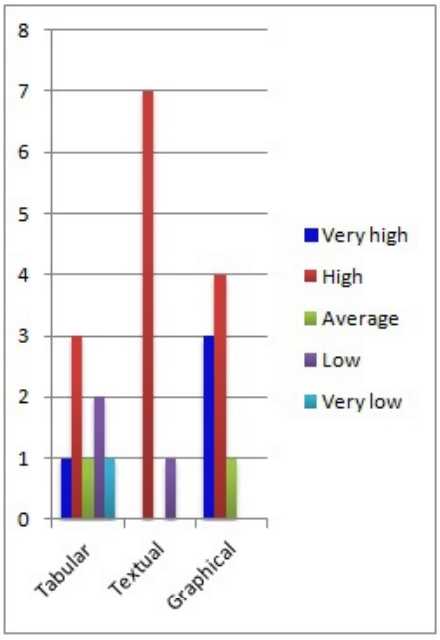

Figure 5.15 – Comparison of Results for Usefulness of Presented Data

The usefulness of presented tabular data ranges from very low through very high, while textual results are mostly high and graphical results are mostly high or very high.

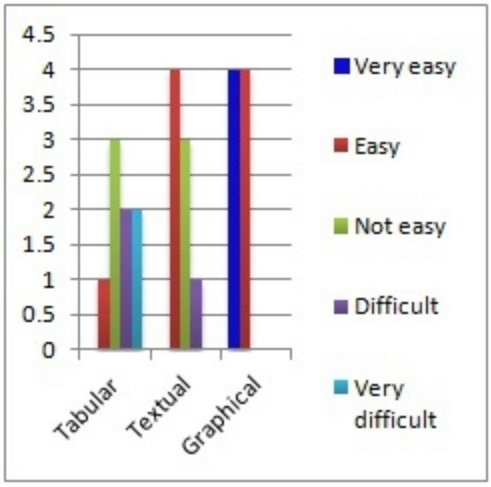

Figure 5.16 – Comparison of Results for Ease of Determining Potential or Motive for Improper Information Sharing or Unauthorized Access

When provided with tabular data, determining potential or motive for improper information sharing is mostly not easy, difficult, or very difficult, while it is mostly easy when provided with textual results, and either easy or very easy when presented as graphical results.

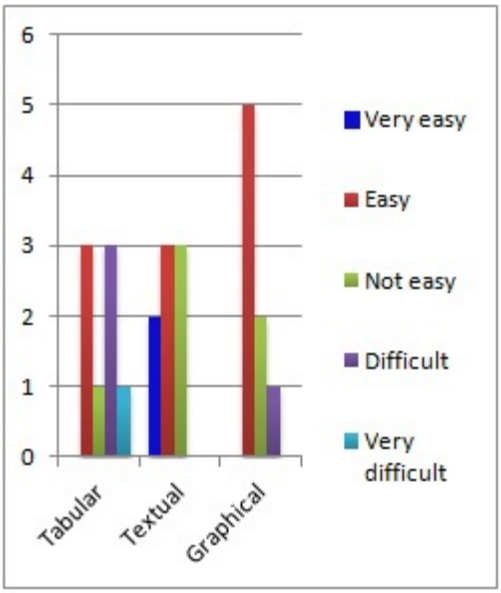

Figure 5.17 – Comparison of Results for Ease of Recognizing Personal Bias

Figure 5.17 shows that the ease of recognizing personal bias the managers or security personnel might have towards an employee ranges from easy through very difficult when provided with tabular data, while it ranges from not easy, easy, or very easy when provided with textual results, and ranges from easy through difficult when provided with graphical results only. The fact that the separate views of automatically monitored, cyber-activity-related data, personally inputted non-cyber-activity-related data, and background information, are only available as textual data explains why it is easier to recognize personal bias using textual results than when using graphical results. Even though the same data is also available in the tabular format, processing that data to glean the relevant information is more cumbersome than when presented as textual results already processed by system.

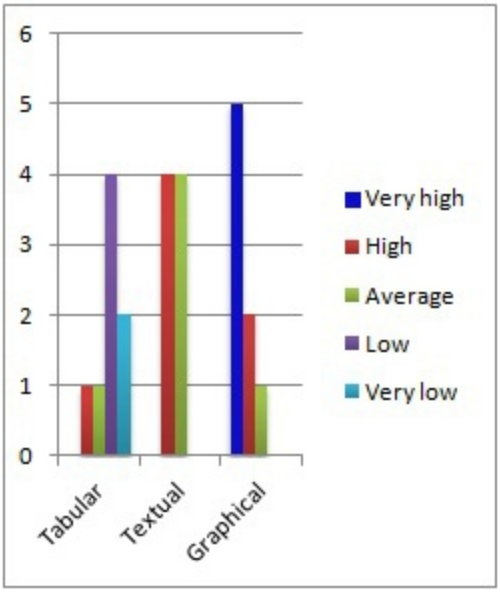

Figure 5.18 – Comparison of Results for Overall Usability of the System

Figure 5.18 shows that the overall usability of tabular data is mostly low, while the overall usability of the system is either high or average when presented as textual results and mostly very high when presented as graphical results.

Figure 5.19 depicts the overall comparison of evaluation results across the three groups. The values for each aspect of evaluation in figure 5.19 were obtained by calculating the weighted mean where “Very poor” = 1 point, “Poor” = 2 points, “Moderate” = 3 points, “Good” = 4 points, and “Very good” = 5 points. As seen through figure 5.19, computing security

behavioural profiles and security education and training schedules manually from tabular data had the lowest usability for each aspect of evaluation. The usability of the system with graphical displays was the highest for all aspects except for the ease of recognizing personal bias. The fact that group C could not view the separate components of cyber activity, non-cyber activity, and background information, explains why the ease of recognizing personal bias for that group was lower than that of group B, which got to view the separate components. Even though tabular data provides the most extensive detail, the difficulty in processing the tabular data resulted in the amount of detail of group A (tabular data) being deemed lower than the amounts for groups B (textual results) and C (graphical results), which got to view already processed information in a clear, concise form.

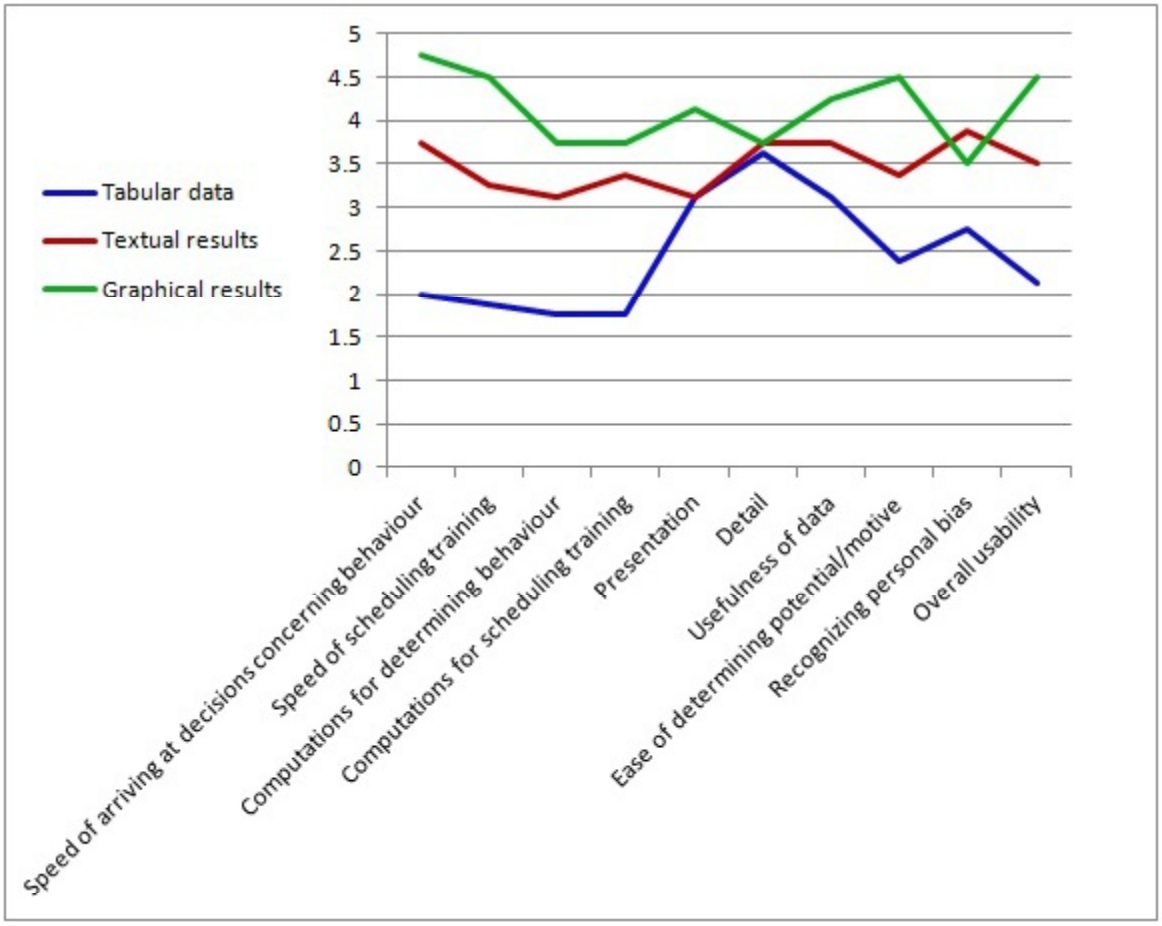

Figure 5.19 – Comparison of Evaluation Results across Groups

These usability evaluation results show that the developed system certainly provides convenience to the ISO and security managers by profiling the security behaviour of

employees of the organization and scheduling security education and training for them. Thus, it also improves the ease and speed of making decisions by the ISO and security managers by presenting these security behavioural profiles and security education and training schedules in a well-organized, user-friendly manner. The fact that group C found it more difficult to recognize personal bias than did group B shows that while the graphical displays project the message in a fast, concise manner, the textual profiles provide further depth and insight into each behavioural characteristic or security infraction. Thus, the graphical results provided by the system should be used in conjunction with the textual results for optimum usability.

5.4 Discussion

It can be seen that the profiling system presented through this research provides a convenient and workable solution to predicting information security behaviour of employees of an organization. By examining the automatically monitored cyber activities, personally observed non-cyber activities, and background information of the employees, the system compiles security behavioural profiles showing which of the employees could potentially engage in which security infractions. Accordingly, the system also determines and schedules the level and type of security education and training to be given to each individual employee. The system presents the behavioural profiles and security education and training schedules in a convenient, timely, and user-friendly fashion to enable faster decision-making by information security officers and security managers.

Through the results of the usability evaluation of this system, it can be seen that this system provides considerable convenience and ease to the information security officers and security managers in making decisions concerning the security behaviour of the organization's employees, the resulting information security problems, and the security training and education to be given to them. The system conveys the messages in a fast, concise manner through its graphical results, while providing more depth and insight into each security behavioural characteristic and security infraction through its textual results.

Chapter 6

Summary

Chapter 6

Summary

6.1 Introduction

Human errors constitute the majority of identified information security breaches and most present-day attacks require a human element to be completed successfully and involve tricking people into revealing confidential information. Most information security attacks originate from the inside with the involvement of trusted insiders. Even though, effective information security requires not only physical and technical controls, but also operational controls concerning the behaviour and actions of employees, most information security systems automatically assume employees' adherence to policies instead of ensuring it. Thus, despite the overall understanding that the human factor should be taken into consideration in ISM, most security solutions available today still rely on purely technical measures to enforce information security. Yet, people may easily bypass technological controls and restrictions by revealing their authentication information to others. Although most technical security measures may be somewhat sufficient to keep outside attacks at bay, these alone are clearly insufficient to ward of insider attacks.

This research addresses the problem of improper sharing of information within an organization, by authorized insiders, with outsiders or unauthorized insiders, and presents a managerial solution blending social and technological methods and techniques together.

Human behaviour is performed according to the personality of the individual and can thus be categorized. The system presented in this paper adapts behavioural profiling, a technique somewhat similar to criminal profiling, by classifying behavioural patterns and predicting the next move. The system detects the level of observance of security best practices and behavioural patterns of employees in an organization by monitoring their cyber and non-cyber activities, and uses this information in combination with their background information

and job details to create security behavioural profiles, in order to provide suggestions to the information security officer and security managers to help them identify users whose actions could potentially lead to information security infractions and ISM problems. Accordingly, the system also determines the level of security education and training required by each individual user and schedules these training programmes.

6.2 Conclusions

In conclusion, it can be stated that the profiling system presented through this research provides a convenient and workable solution to achieve internal control of information sharing within an organization by profiling and thereby predicting information security behaviour of its employees.

This system employs both social and technological information gathering methods by allowing observable information about employees' non-cyber-activity-related behaviour to be inputted personally by managers and security personnel, and through the automatic monitoring of cyber activities. It also provides a managerial solution, which employs a mixture of technological and social methods and techniques to this human-related information security problem of improper information sharing by providing automatic access control, scheduling security education and training, etc., along with hands on security awareness and training workshops conducted by security professionals, and allowing the use of personal judgement by the ISO, etc., and thereby, overcoming the weaknesses of a purely technological solution.

Even though the monitoring of employees' activities would normally produce privacy implications, this system keeps such implications to a minimal by providing the two separate "strict" and "relaxed" modes to clearly distinguish the times when monitoring of activities will or will not be conducted.

Finally, by allowing the ISO to configure the security behavioural rules to be aligned with the business objectives of the organization, this system can be tailor-made to suit the specific requirements of the organization.

Through the results obtained by testing the system presented above with the hypothetical test cases, it can be stated that the implemented system accurately computes cyber activity. The resulting profiles of both hypothetical and real-life test cases prove that this system can be used for accurate profiling of security behaviour and effective prediction of security infractions and information security behavioural flaws by employees within an organization to a certain extent.

Through the results of the usability evaluation of this system, it can be stated that this system provides considerable convenience and ease to the information security officers and security managers in making decisions concerning the security behaviour of the organization's employees and the security training and education to be given to them. The system conveys the messages in a fast, concise manner through its graphical results, while providing more depth and insight into each security behavioural characteristic and security infraction through its textual results.

6.3 Future Work

As future work, currently existing common algorithms could be reused with modifications and integrated to the implementation of this system to cover all the areas of monitoring of security behaviour proposed through this research.

In addition, the system could be deployed and put to use on real people in order to obtain real test results to further evaluate the system's functionality.

The profiling system could also be expanded to include features such as:

- Allowing the dynamic addition of new security rules by the information security officer to the rule base of the inference system
- Prioritizing security infractions / behavioural flaws

- Observing employees' security behaviour over a period of time and reporting the information security problems / security infractions which are most common or which are most likely to occur in the foreseeable future
- Group-wise viewing of security behavioural problems and security education and training schedules

References

References by Name

American Association for the Advancement of Science (1990). Chapter 7: Human society. Available at http://www.project2061.org/publications/sfaa/online/chap7.htm (accessed 22 November 2011).

Asai, T. (2007). *Information Security and Business Activities*. Niigata, Japan: Kameda Book Service.

Asai, T. and Fernando, S. (2011_a). Human-related problems in information security in Indian cross-cultural environments. *Journal of Japan Society of Security Management, 25(2),* 3-14.

Asai, T. and Fernando, S. (2011_b). Human-related problems in information security in Thai cross-cultural environments. *International Journal of Contemporary Management Research, 7(2),* 117-141.

Asai, T., Fernando, S. and Castillo, J. (2011). Human-related problems in information security in Russian cross-cultural environments. *International Journal of Japan Association of Management Systems, 3(1),* 31-40.

Bean, M. (2008). *Human Error at the Centre of IT Security Breaches*. Retrieved from http://www.newhorizons.com/elevate/network%20defence%20contributed%20article.pdf (accessed 10 February 2008).

Bishop, M. (2003). *Computer Security – Art and Science*. Boston, MA: Addison-Wesley.

Claridge, J. (2012). Criminal profiling and its use in crime solving. Retrieved from http://www.exploreforensics.co.uk/criminal-profiling-and-its-use-in-crime-solving.html (accessed 12 April 2012).

Committee of Sponsoring Organizations. (1994). *Internal Control – Integrated Framework*. Retrieved from http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf (accessed 17 February 2008).

Duda, R.O., Hart, P.E., Nilsson, N.J. and Sutherland, G.L. (1977). Semantic network representations in rule-based inference systems. *Technical Note 136, Artificial Intelligence Center*. Retrieved from http://www.sri.com/sites/default/files/uploads/publications/pdf/751.pdf (accessed 12 March 2014)

Enterra Solutions (2014). Rules-based inference systems. Enterra Insights Blog. Retrieved from http://www.enterrasolutions.com/products/inference (accessed on 12 March 2014)

Fernando, S. and Asai, T. (2011_a). Information security problems faced by American companies in economically rising countries. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Fernando, S. and Asai, T. (2011_b). Human-related information security problems faced by British companies in economically rising countries. *Proceedings of the 9th Australian Information Security Management Conference, Perth, Western Australia.*

Foley, K. (2011). Maintaining a proactive and sustainable security program while hosting and processing personally identifiable information. *Information Systems Security Association Journal, 9 (5),* 25-32.

Gonzalez, J.J. and Sawicka, A. (2002). A framework for human factors in information security. *Proceedings of 2002 World Scientific and Engineering Academic Society International Conference on Information Security, Rio de Janeiro*.

Griffin, N.L. and Lewis, F. D. (1989). A rule-based inference engine which is optimal and VLSI implementable. Department of Computer Science, University of Kentucky, Lexington, Kentucky 40506, Retrieved from http://www.cs.uky.edu/~lewis/papers/inf-engine.pdf (accessed 12 March 2014)

Grimes, R. A. (2010). How to thwart employee cybercrime. *Insider Threat Deep Drive – Combating the Enemy Within, InfoWorld – Special Report*, 2-7. Retrieved from http://resources.idgenterprise.com/original/AST-0001528_insiderthreat_2_v1.pdf (accessed 5 August 2012).

Harris, M. and Patten, K. (2011). Managing corporate computer crime and the insider threat: the role of cognitive dissonance theory. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Harris, S. (2004). *All in One CISSP Certification: Exam Study Guide* (2nd Ed.). Berkeley, CA: Osborne/McGraw Hill.

Insight Express. (2008). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved from CISCO Systems, Inc. http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/data-loss-prevention/Cisco_STL_Data_Leakage_2008_.pdf (accessed 15 November 2011).

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: ISO.

Kahneman, D. and Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Economoetrica*, 47, 263-291. http://dx.doi.org/10.2307/1914185

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Liu, A., Martin, C., Hetherington, T. and Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. *Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY*.

Lynch, D. M. (2006). Securing against insider attacks. *Information Security and Risk Management*, 39-47. Retrieved from http://www.csb.uncw.edu/people/ivancevichd/classes/MSA%20516/Supplemental%20Readings/Supplemental%20Reading%20for%20Wed,%2011-5/Insider%20Attacks.pdf (accessed 5 August 2012).

Mills, R.F., Grimaila, M.R., Peterson, G.L. and Butts, J.W. (2011). A scenario-based approach to mitigating the insider threat. *Information Systems Security Association Journal, 9 (5)*, 12-19.

Ning, P., Jajodia, S. and Wang, X.S. (2003). *Intrusion Detection in Distributed Systems – An Abstraction-Based Approach*. Norwell, MA: Kluwer Academic Publishers.

Okayasu, K. (2014). Cognitive dissonance: information security and whistle blowers. *Journal of Japan Society of Security Management, 27 (3)*, 35-40.

Peltier, T.R. (2002). *Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL: Auerback Publications.

Platt, J. (2000). Rule-based systems. University of the Aegean, Greece. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CFEQFjAF&url=http%3A%2F%2Fwww.icsd.aegean.gr%2Flecturers%2Fkonsterg%2Fteaching%2FKE%2FRules.ppt&ei=tfQfU6-tAcrGkgWnYFw&usg=AFQjCNGrD893MbpbE4pncYs6ArULyzR_uQ&bvm=bv.62788935,d.dGI (accessed 12 March 2014)

Pronin, E. (2006). Perception and misperception of bias in human judgement. *Journal of Trends in Cognitive Sciences, 11,* 37-43. doi:10-1016/j.tics.2006.11.001

Sabett, R.V. (2011). Have you seen the latest and greatest "security game changer"? *Journal of Information Systems Security Association, 9 (5),* 5.

Schneier, B. (2008). *The psychology of security*. Retrieved from http://www.schneier.com/essay-155.html (accessed 22 November 2011).

Schweitzer, J. A. (1996). *Protecting Business Information*. Newton, MA: Butterworth-Heinemann.

Thapar, A. (2007). Social engineering: an attack vector most intricate to tackle. *White paper*. Retrieved from http://www.infosecwriters.com/texts.php?op=display&id=564 (accessed on 15 November 2011).

The Myers & Briggs Foundation. *MBTI basics*. Retrieved from http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/ (accessed on 15 March 2012).

Thompson, M. (2011). *An introduction to behavioural evidence analysis*. Retrieved from http://colbycriminaljustice.wikidot.com/criminal-profiling (accessed 12 April 2012).

Turvey, B. (2000). Criminal profiling: an introduction to behavioural evidence analysis. *The American Journal of Psychiatry, 157,* 1532-1534. doi:10.1176/appi.ajp.157.9.1532

Vroom, C. and von Solms, R. (2003), Information Security: Auditing the Behaviour of the Employee. *IFIP TC11 18th International Conference on Information Security (SEC2003),* Athens, Greece. In Gritzalis, D., De Capitani di Vimercati, S., Samarati, P. and Katsikas, S. (Ed.), *Security and Privacy in the Age of Uncertainty* (pp. 401-404). Norwell, MA: Kluwer Academic Publishers.

West, R. (2008) The psychology of security. *Communications of the Association for Computing Machinery,* 51(4), 34-41. http://dx.doi.org/10.1145.1330311.1330320

Williams, B. R. (2011), Do it differently, *Journal of Information Systems Security Association, 9 (5),* 6.

Winerman, L. (2004). Criminal profiling: the reality behind the myth. *American Psychological Association, 35 (7),* 66-69.

Young, T.M. and Varano, S. (2006). *Profiling pros and cons: an evaluation of contemporary criminal profiling methodologies*. Final report – Honours Program. Northeastern University, Boston, MA.

References by Appearance

Bishop, M. (2003). *Computer Security – Art and Science*. Boston, MA: Addison-Wesley.

Harris, S. (2004). *All in One CISSP Certification: Exam Study Guide* (2nd Ed.). Berkeley, CA: Osborne/McGraw Hill.

Asai, T. (2007). *Information Security and Business Activities*. Niigata, Japan: Kameda Book Service.

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: ISO.

Committee of Sponsoring Organizations. (1994). *Internal Control – Integrated Framework*. Retrieved from http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf (accessed 17 February 2008).

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Vroom, C. and von Solms, R. (2003), Information Security: Auditing the Behaviour of the Employee. *IFIP TC11 18th International Conference on Information Security (SEC2003)*, Athens, Greece. In Gritzalis, D., De Capitani di Vimercati, S., Samarati, P. and Katsikas, S. (Ed.), *Security and Privacy in the Age of Uncertainty* (pp. 401-404). Norwell, MA: Kluwer Academic Publishers.

Schweitzer, J. A. (1996). *Protecting Business Information*. Newton, MA: Butterworth-Heinemann.

Bean, M. (2008). *Human Error at the Centre of IT Security Breaches*. Retrieved from http://www.newhorizons.com/elevate/network%20defence%20contributed%20article.pdf (accessed 10 February 2008).

Asai, T. and Fernando, S. (2011_a). Human-related problems in information security in Indian cross-cultural environments. *Journal of Japan Society of Security Management, 25(2),* 3-14.

Asai, T., Fernando, S. and Castillo, J. (2011). Human-related problems in information security in Russian cross-cultural environments. *International Journal of Japan Association of Management Systems, 3(1),* 31-40.

Fernando, S. and Asai, T. (2011_a). Information security problems faced by American companies in economically rising countries. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Fernando, S. and Asai, T. (2011_b). Human-related information security problems faced by British companies in economically rising countries. *Proceedings of the 9th Australian Information Security Management Conference, Perth, Western Australia.*

Asai, T. and Fernando, S. (2011_b). Human-related problems in information security in Thai cross-cultural environments. *International Journal of Contemporary Management Research, 7(2),* 117-141.

Insight Express. (2008). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved from CISCO Systems, Inc. http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/data-loss-prevention/Cisco_STL_Data_Leakage_2008_.pdf (accessed 15 November 2011).

Pronin, E. (2006). Perception and misperception of bias in human judgement. *Journal of Trends in Cognitive Sciences, 11,* 37-43. doi:10-1016/j.tics.2006.11.001

Schneier, B. (2008). *The psychology of security*. Retrieved from http://www.schneier.com/essay-155.html (accessed 22 November 2011).

Williams, B. R. (2011), Do it differently, *Journal of Information Systems Security Association, 9 (5),* 6.

Lynch, D. M. (2006). Securing against insider attacks. *Information Security and Risk Management*, 39-47. Retrieved from http://www.csb.uncw.edu/people/ivancevichd/classes/MSA%20516/Supplemental%20Readings/Supplemental%20Reading%20for%20Wed,%2011-5/Insider%20Attacks.pdf (accessed 5 August 2012).

Grimes, R. A. (2010). How to thwart employee cybercrime. *Insider Threat Deep Drive – Combating the Enemy Within, InfoWorld – Special Report*, 2-7. Retrieved from http://resources.idgenterprise.com/original/AST-0001528_insiderthreat_2_v1.pdf (accessed 5 August 2012).

Ning, P., Jajodia, S. and Wang, X.S. (2003). *Intrusion Detection in Distributed Systems – An Abstraction-Based Approach*. Norwell, MA: Kluwer Academic Publishers.

Liu, A., Martin, C., Hetherington, T. and Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. *Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.*

Mills, R.F., Grimaila, M.R., Peterson, G.L. and Butts, J.W. (2011). A scenario-based approach to mitigating the insider threat. *Information Systems Security Association Journal, 9 (5)*, 12-19.

Sabett, R.V. (2011). Have you seen the latest and greatest "security game changer"? *Journal of Information Systems Security Association, 9 (5)*, 5.

Foley, K. (2011). Maintaining a proactive and sustainable security program while hosting and processing personally identifiable information. *Information Systems Security Association Journal, 9 (5)*, 25-32.

Gonzalez, J.J. and Sawicka, A. (2002). A framework for human factors in information security. *Proceedings of 2002 World Scientific and Engineering Academic Society International Conference on Information Security, Rio de Janeiro*.

Peltier, T.R. (2002). *Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL: Auerback Publications.

Young, T.M. and Varano, S. (2006). *Profiling pros and cons: an evaluation of contemporary criminal profiling methodologies*. Final report – Honours Program. Northeastern University, Boston, MA.

Thompson, M. (2011). *An introduction to behavioural evidence analysis*. Retrieved from http://colbycriminaljustice.wikidot.com/criminal-profiling (accessed 12 April 2012).

Claridge, J. (2012). Criminal profiling and its use in crime solving. Retrieved from http://www.exploreforensics.co.uk/criminal-profiling-and-its-use-in-crime-solving.html (accessed 12 April 2012).

Winerman, L. (2004). Criminal profiling: the reality behind the myth. *American Psychological Association, 35 (7)*, 66-69.

Turvey, B. (2000). Criminal profiling: an introduction to behavioural evidence analysis. *The American Journal of Psychiatry, 157*, 1532-1534. doi:10.1176/appi.ajp.157.9.1532

American Association for the Advancement of Science (1990). Chapter 7: Human society. Available at http://www.project2061.org/publications/sfaa/online/chap7.htm (accessed 22 November 2011).

West, R. (2008) The psychology of security. *Communications of the Association for Computing Machinery*, 51(4), 34-41. http://dx.doi.org/10.1145.1330311.1330320

Kahneman, D. and Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Economoetrica*, 47, 263-291. http://dx.doi.org/10.2307/1914185

The Myers & Briggs Foundation. *MBTI basics*. Retrieved from http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/ (accessed on 15 March 2012).

Enterra Solutions (2014). Rules-based inference systems. Enterra Insights Blog. Retrieved from http://www.enterrasolutions.com/products/inference (accessed on 12 March 2014)

Griffin, N.L. and Lewis, F. D. (1989). A rule-based inference engine which is optimal and VLSI implementable. Department of Computer Science, University of Kentucky, Lexington, Kentucky 40506, Retrieved from http://www.cs.uky.edu/~lewis/papers/inf-engine.pdf (accessed 12 March 2014)

Platt, J. (2000). Rule-based systems. University of the Aegean, Greece. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CFEQFjAF&url=http%3A%2F%2Fwww.icsd.aegean.gr%2Flecturers%2Fkonsterg%2Fteaching%2FKE%2FRules.ppt&ei=tfQfU6-tAcrGkgW-nYFw&usg=AFQjCNGrD893MbpbE4pncYs6ArULyzR_uQ&bvm=bv.62788935,d.dGI (accessed 12 March 2014)

Duda, R.O., Hart, P.E., Nilsson, N.J. and Sutherland, G.L. (1977). Semantic network representations in rule-based inference systems. *Technical Note 136, Artificial Intelligence Center*. Retrieved from http://www.sri.com/sites/default/files/uploads/publications/pdf/751.pdf (accessed 12 March 2014)

Thapar, A. (2007). Social engineering: an attack vector most intricate to tackle. *White paper*. Retrieved from http://www.infosecwriters.com/texts.php?op=display&id=564 (accessed on 15 November 2011).

Harris, M. and Patten, K. (2011). Managing corporate computer crime and the insider threat: the role of cognitive dissonance theory. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Okayasu, K. (2014). Cognitive dissonance: information security and whistle blowers. *Journal of Japan Society of Security Management, 27 (3)*, 35-40.

References by Year

Duda, R.O., Hart, P.E., Nilsson, N.J. and Sutherland, G.L. (1977). Semantic network representations in rule-based inference systems. *Technical Note 136, Artificial Intelligence Center.* Retrieved from http://www.sri.com/sites/default/files/uploads/publications/pdf/751.pdf (accessed 12 March 2014)

Kahneman, D. and Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Economoetrica*, 47, 263-291. http://dx.doi.org/10.2307/1914185

Griffin, N.L. and Lewis, F. D. (1989). A rule-based inference engine which is optimal and VLSI implementable. Department of Computer Science, University of Kentucky, Lexington, Kentucky 40506, Retrieved from http://www.cs.uky.edu/~lewis/papers/inf-engine.pdf (accessed 12 March 2014)

American Association for the Advancement of Science (1990). Chapter 7: Human society. Available at http://www.project2061.org/publications/sfaa/online/chap7.htm (accessed 22 November 2011).

Committee of Sponsoring Organizations. (1994). *Internal Control – Integrated Framework.* Retrieved from http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf (accessed 17 February 2008).

Schweitzer, J. A. (1996). *Protecting Business Information*. Newton, MA: Butterworth-Heinemann.

Platt, J. (2000). Rule-based systems. University of the Aegean, Greece. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CFEQFjAF&url=http%3A%2F%2Fwww.icsd.aegean.gr%2Flecturers%2Fkonsterg%2Fteaching%2FKE%2FRules.ppt&ei=tfQfU6-tAcrGkgW-nYFw&usg=AFQjCNGrD893MbpbE4pncYs6ArULyzR_uQ&bvm=bv.62788935,d.dGI (accessed 12 March 2014)

Turvey, B. (2000). Criminal profiling: an introduction to behavioural evidence analysis. *The American Journal of Psychiatry, 157*, 1532-1534. doi:10.1176/appi.ajp.157.9.1532

Gonzalez, J.J. and Sawicka, A. (2002). A framework for human factors in information security. *Proceedings of 2002 World Scientific and Engineering Academic Society International Conference on Information Security, Rio de Janeiro*.

Peltier, T.R. (2002). *Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL: Auerback Publications.

Bishop, M. (2003). *Computer Security – Art and Science*. Boston, MA: Addison-Wesley.

Ning, P., Jajodia, S. and Wang, X.S. (2003). *Intrusion Detection in Distributed Systems – An Abstraction-Based Approach*. Norwell, MA: Kluwer Academic Publishers.

Vroom, C. and von Solms, R. (2003), Information Security: Auditing the Behaviour of the Employee. *IFIP TC11 18th International Conference on Information Security (SEC2003)*, Athens, Greece. In Gritzalis, D., De Capitani di Vimercati, S., Samarati, P. and Katsikas, S. (Ed.), *Security and Privacy in the Age of Uncertainty* (pp. 401-404). Norwell, MA: Kluwer Academic Publishers.

Harris, S. (2004). *All in One CISSP Certification: Exam Study Guide* (2nd Ed.). Berkeley, CA: Osborne/McGraw Hill.

Winerman, L. (2004). Criminal profiling: the reality behind the myth. *American Psychological Association, 35 (7),* 66-69.

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: ISO.

Liu, A., Martin, C., Hetherington, T. and Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. *Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY*.

Lynch, D. M. (2006). Securing against insider attacks. *Information Security and Risk Management*, 39-47. Retrieved from http://www.csb.uncw.edu/people/ivancevichd/classes/MSA%20516/Supplemental%20Readings/Supplemental%20Reading%20for%20Wed,%2011-5/Insider%20Attacks.pdf (accessed 5 August 2012).

Pronin, E. (2006). Perception and misperception of bias in human judgement. *Journal of Trends in Cognitive Sciences, 11,* 37-43. doi:10-1016/j.tics.2006.11.001

Young, T.M. and Varano, S. (2006). *Profiling pros and cons: an evaluation of contemporary criminal profiling methodologies*. Final report – Honours Program. Northeastern University, Boston, MA.

Asai, T. (2007). *Information Security and Business Activities*. Niigata, Japan: Kameda Book Service.

Thapar, A. (2007). Social engineering: an attack vector most intricate to tackle. *White paper*. Retrieved from http://www.infosecwriters.com/texts.php?op=display&id=564 (accessed on 15 November 2011).

Bean, M. (2008). *Human Error at the Centre of IT Security Breaches*. Retrieved from http://www.newhorizons.com/elevate/network%20defence%20contributed%20article.pdf (accessed 10 February 2008).

Insight Express. (2008). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved from CISCO Systems, Inc. http://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/data-loss-prevention/Cisco_STL_Data_Leakage_2008_.pdf (accessed 15 November 2011).

Schneier, B. (2008). *The psychology of security*. Retrieved from http://www.schneier.com/essay-155.html (accessed 22 November 2011).

West, R. (2008) The psychology of security. *Communications of the Association for Computing Machinery,* 51(4), 34-41. http://dx.doi.org/10.1145.1330311.1330320

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Grimes, R. A. (2010). How to thwart employee cybercrime. *Insider Threat Deep Drive – Combating the Enemy Within, InfoWorld – Special Report,* 2-7. Retrieved from http://resources.idgenterprise.com/original/AST-0001528_insiderthreat_2_v1.pdf (accessed 5 August 2012).

Asai, T. and Fernando, S. (2011_a). Human-related problems in information security in Indian cross-cultural environments. *Journal of Japan Society of Security Management, 25(2),* 3-14.

Asai, T. and Fernando, S. (2011_b). Human-related problems in information security in Thai cross-cultural environments. *International Journal of Contemporary Management Research, 7(2),* 117-141.

Asai, T., Fernando, S. and Castillo, J. (2011). Human-related problems in information security in Russian cross-cultural environments. *International Journal of Japan Association of Management Systems, 3(1),* 31-40.

Fernando, S. and Asai, T. (2011_a). Information security problems faced by American companies in economically rising countries. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Fernando, S. and Asai, T. (2011_b). Human-related information security problems faced by British companies in economically rising countries. *Proceedings of the 9th Australian Information Security Management Conference, Perth, Western Australia.*

Foley, K. (2011). Maintaining a proactive and sustainable security program while hosting and processing personally identifiable information. *Information Systems Security Association Journal, 9 (5)*, 25-32.

Harris, M. and Patten, K. (2011). Managing corporate computer crime and the insider threat: the role of cognitive dissonance theory. *Proceedings of the 10th Annual Security Conference, Las Vegas, USA.*

Mills, R.F., Grimaila, M.R., Peterson, G.L. and Butts, J.W. (2011). A scenario-based approach to mitigating the insider threat. *Information Systems Security Association Journal, 9 (5)*, 12-19.

Sabett, R.V. (2011). Have you seen the latest and greatest "security game changer"? *Journal of Information Systems Security Association, 9 (5)*, 5.

Thompson, M. (2011). *An introduction to behavioural evidence analysis*. Retrieved from http://colbycriminaljustice.wikidot.com/criminal-profiling (accessed 12 April 2012).

Williams, B. R. (2011), Do it differently, *Journal of Information Systems Security Association, 9 (5)*, 6.

Claridge, J. (2012). Criminal profiling and its use in crime solving. Retrieved from http://www.exploreforensics.co.uk/criminal-profiling-and-its-use-in-crime-solving.html (accessed 12 April 2012).

Enterra Solutions (2014). Rules-based inference systems. Enterra Insights Blog. Retrieved from http://www.enterrasolutions.com/products/inference (accessed on 12 March 2014)

Okayasu, K. (2014). Cognitive dissonance: information security and whistle blowers. *Journal of Japan Society of Security Management, 27 (3)*, 35-40.

The Myers & Briggs Foundation. *MBTI basics*. Retrieved from http://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/ (accessed on 15 March 2012).

Appendices

Appendix A – Graphical User Interfaces

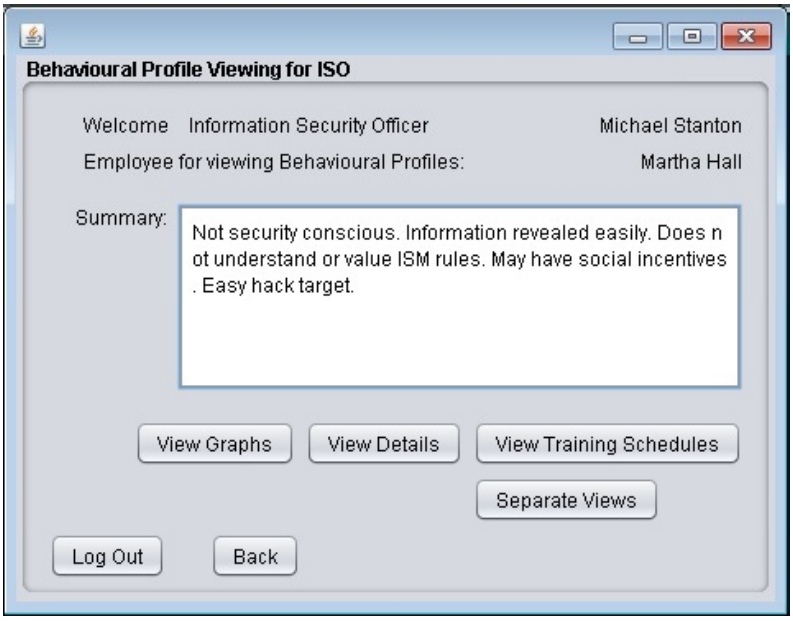

Figure A.1 – Summarized behavioural profile of Martha Hall (Emp0001)

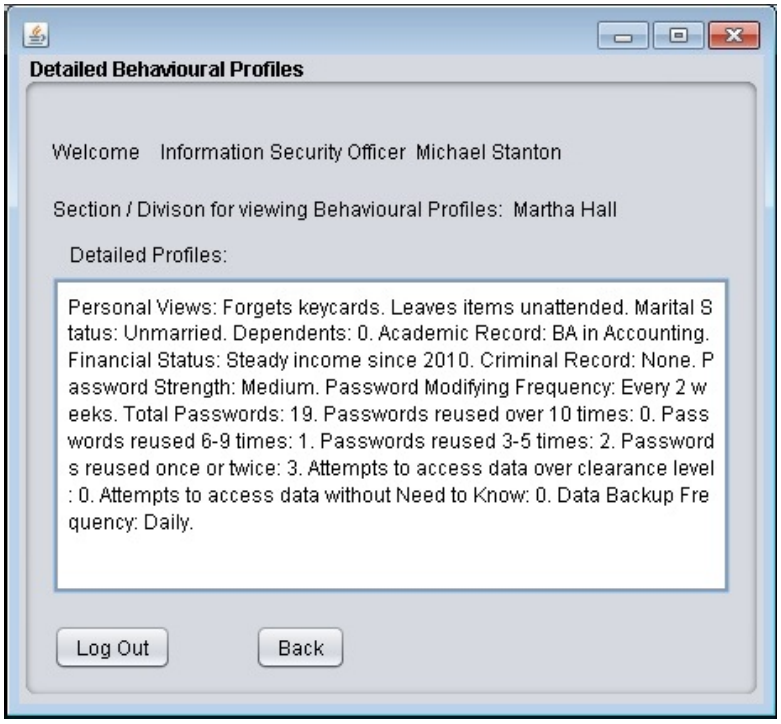

Figure A.2 – Detailed behavioural profile of Martha Hall (Emp0001)

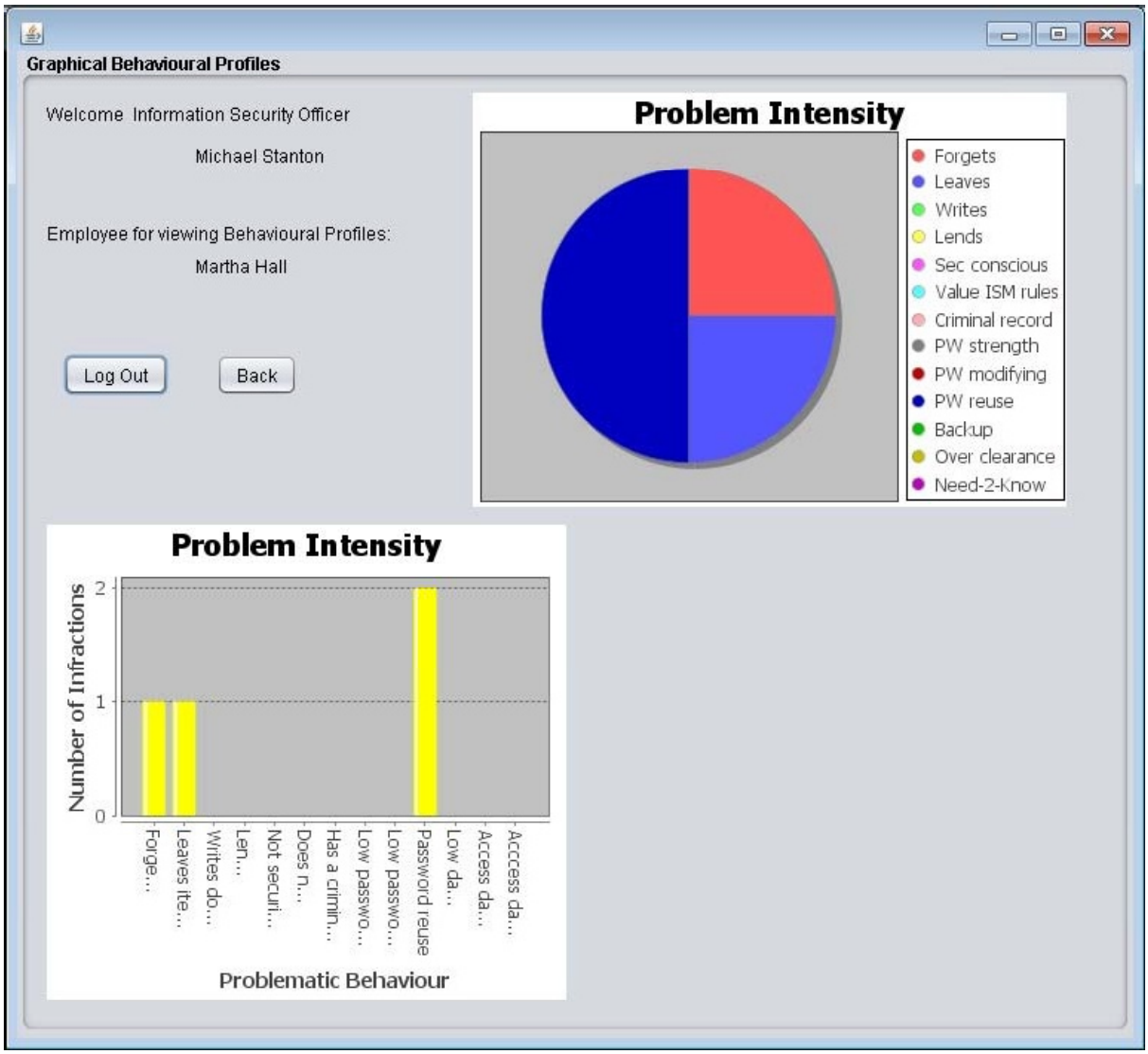

Figure A.3 – Graphical behavioural profile of Martha Hall (Emp0001)

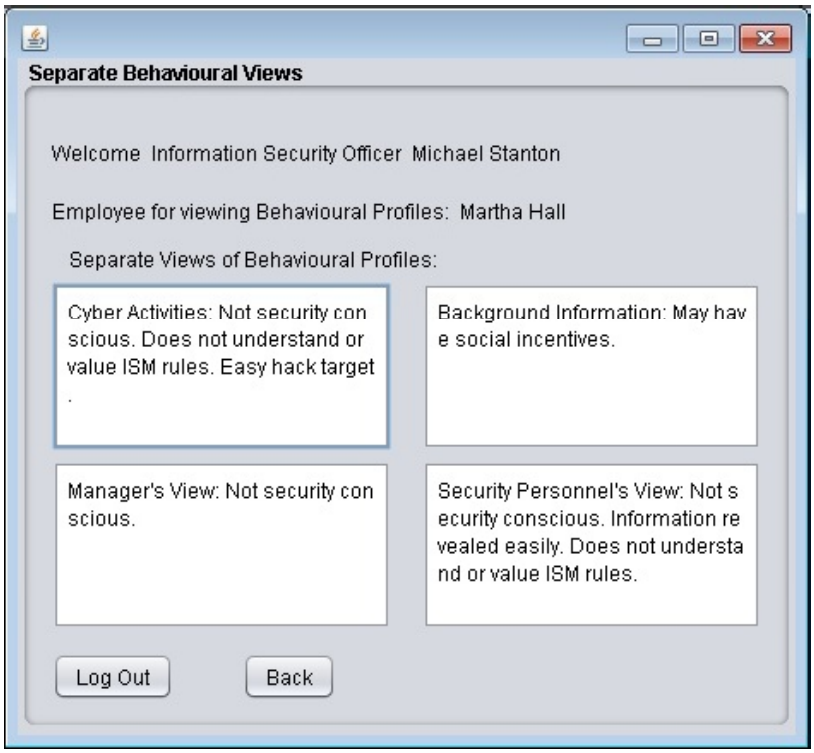

Figure A.4 – Separate views of the behavioural profile of Martha Hall (Emp0001)

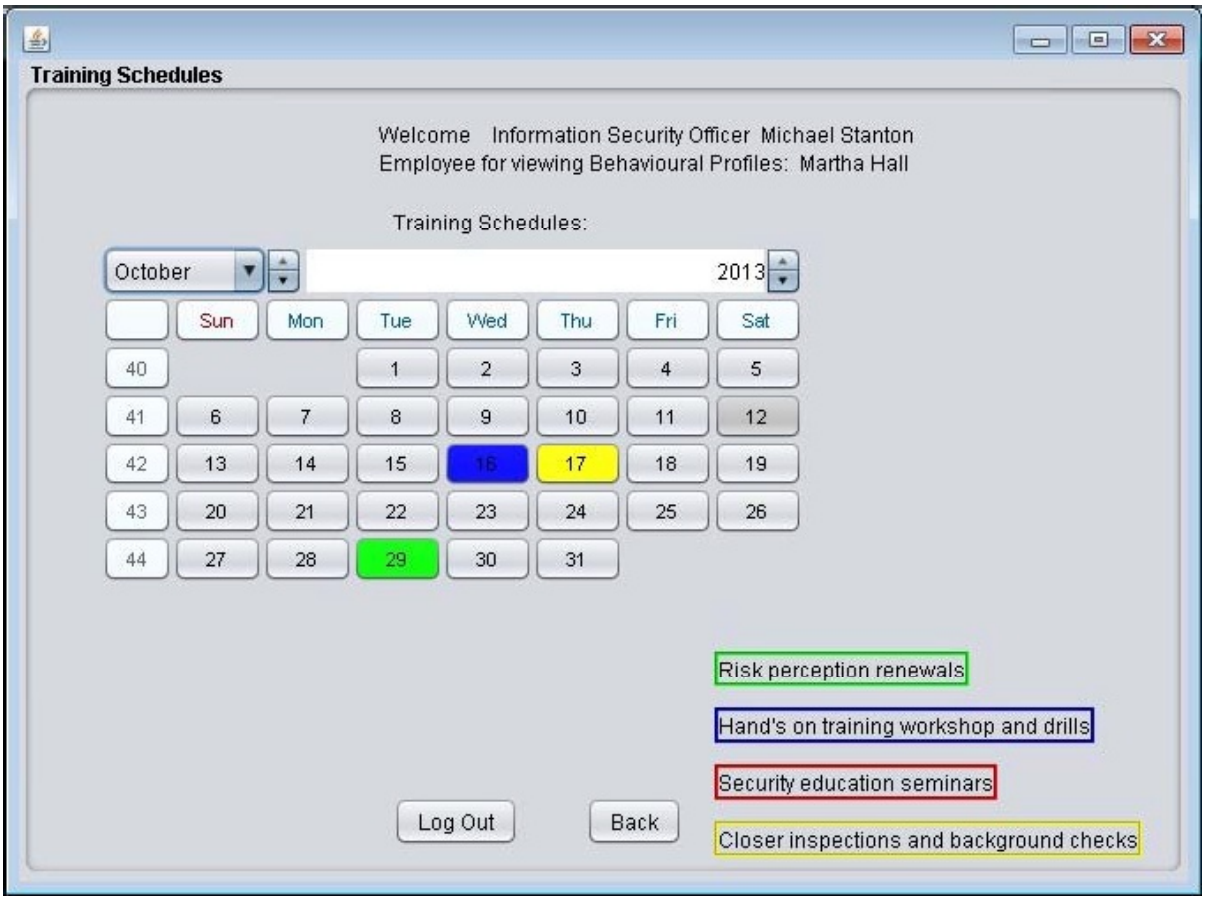

Figure A.5 – Security training schedules for Martha Hall (Emp0001)

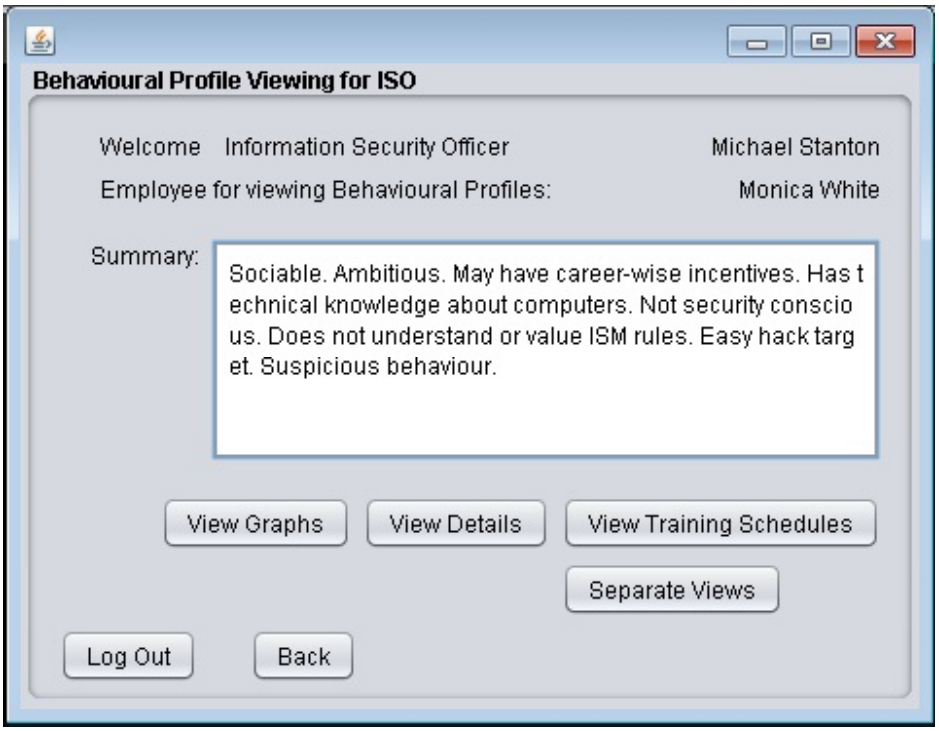

Figure A.6 – Summarized behavioural profile of Monica White (Emp0002)

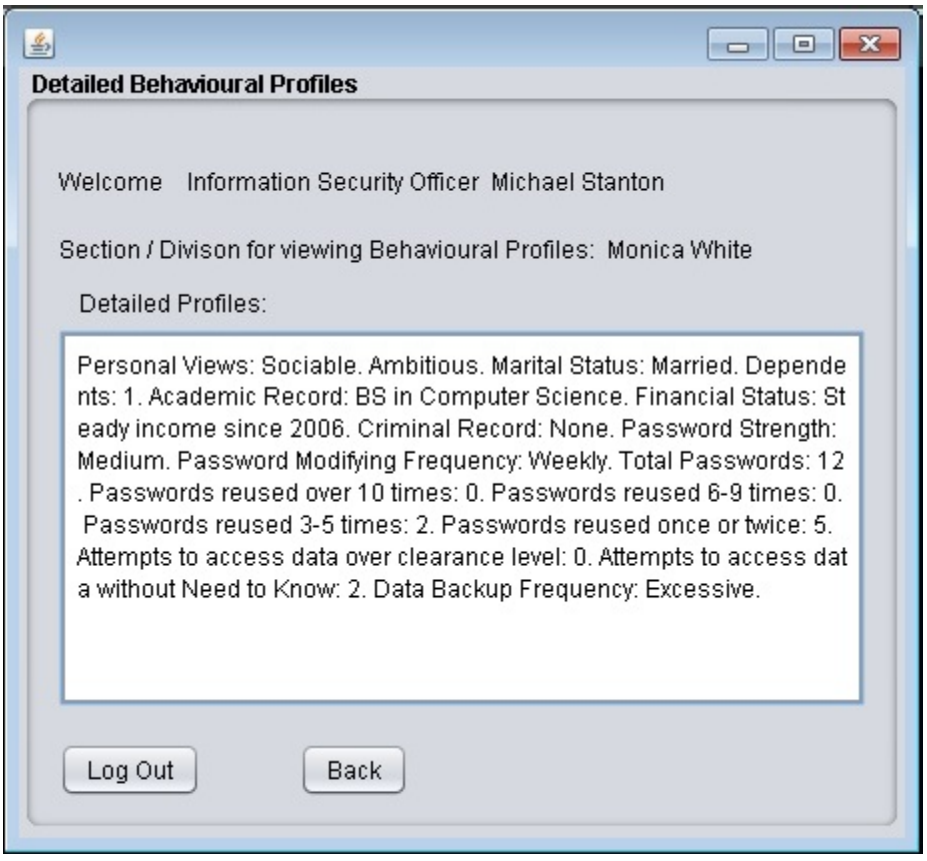

Figure A.7 – Detailed behavioural profile of Monica White (Emp0002)

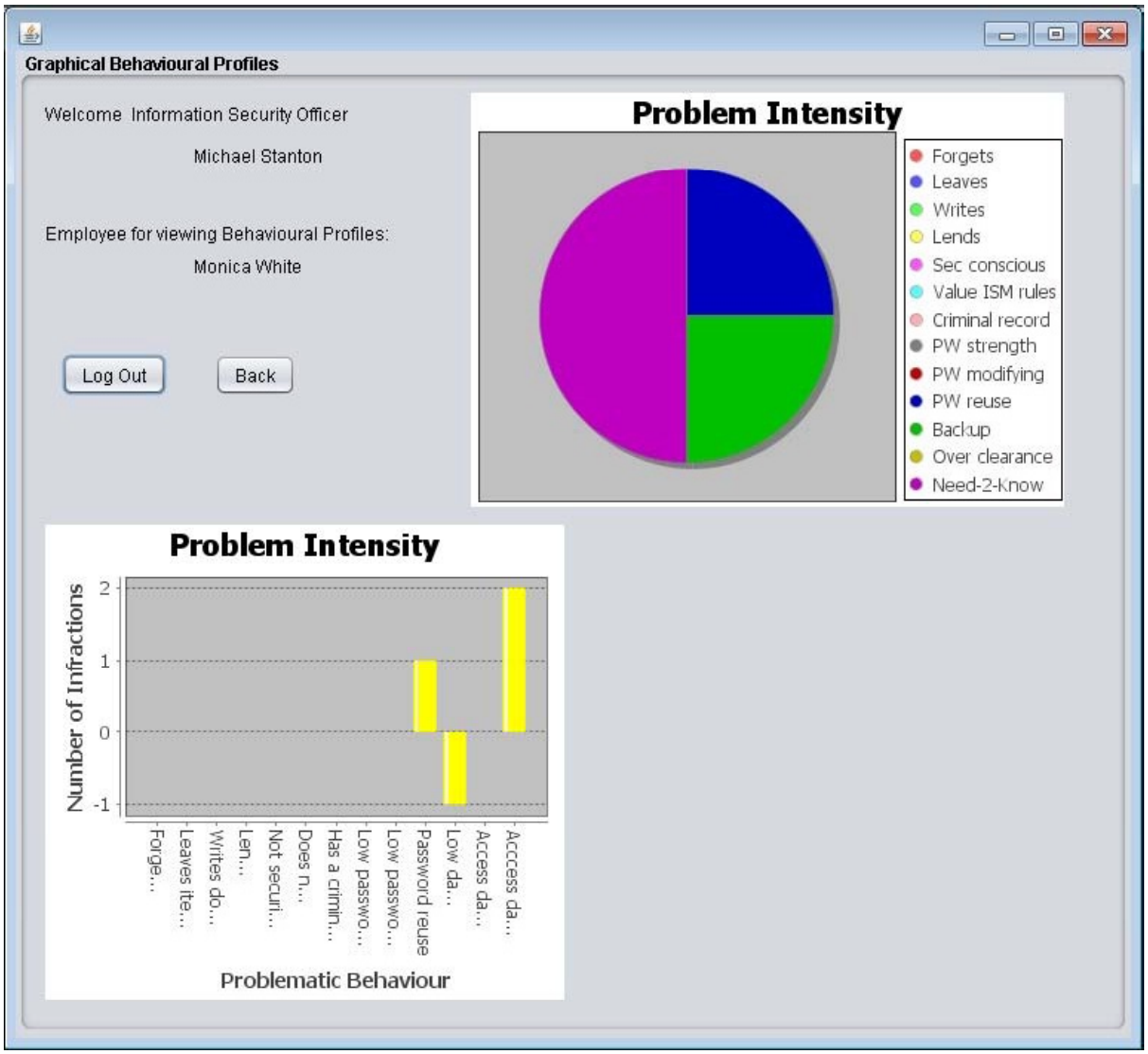

Figure A.8 – Graphical behavioural profile of Monica White (Emp0002)

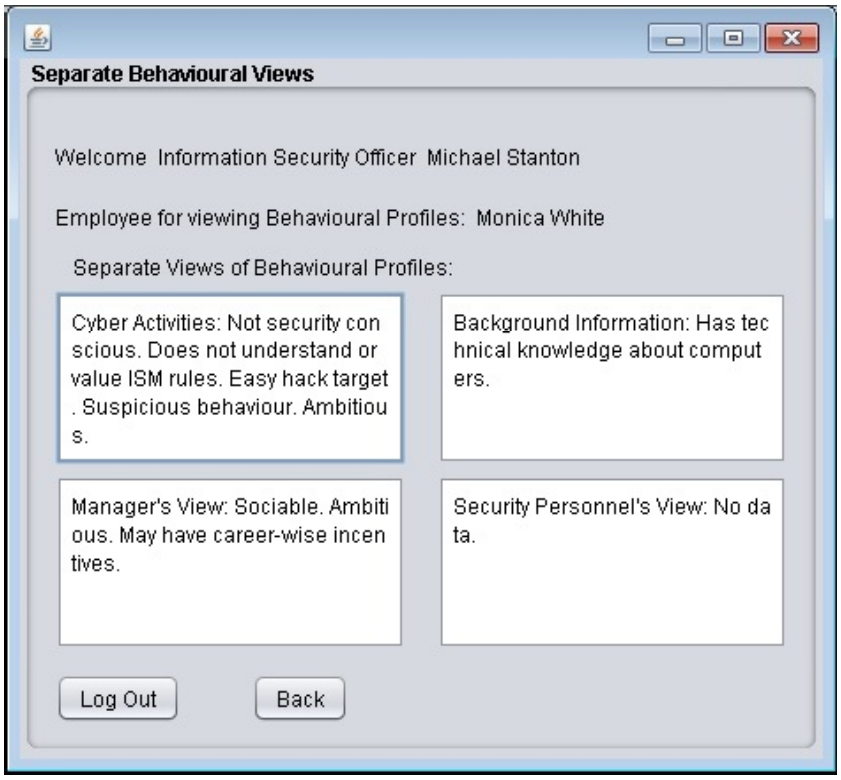

Figure A.9 – Separate views of the behavioural profile of Monica White (Emp0002)

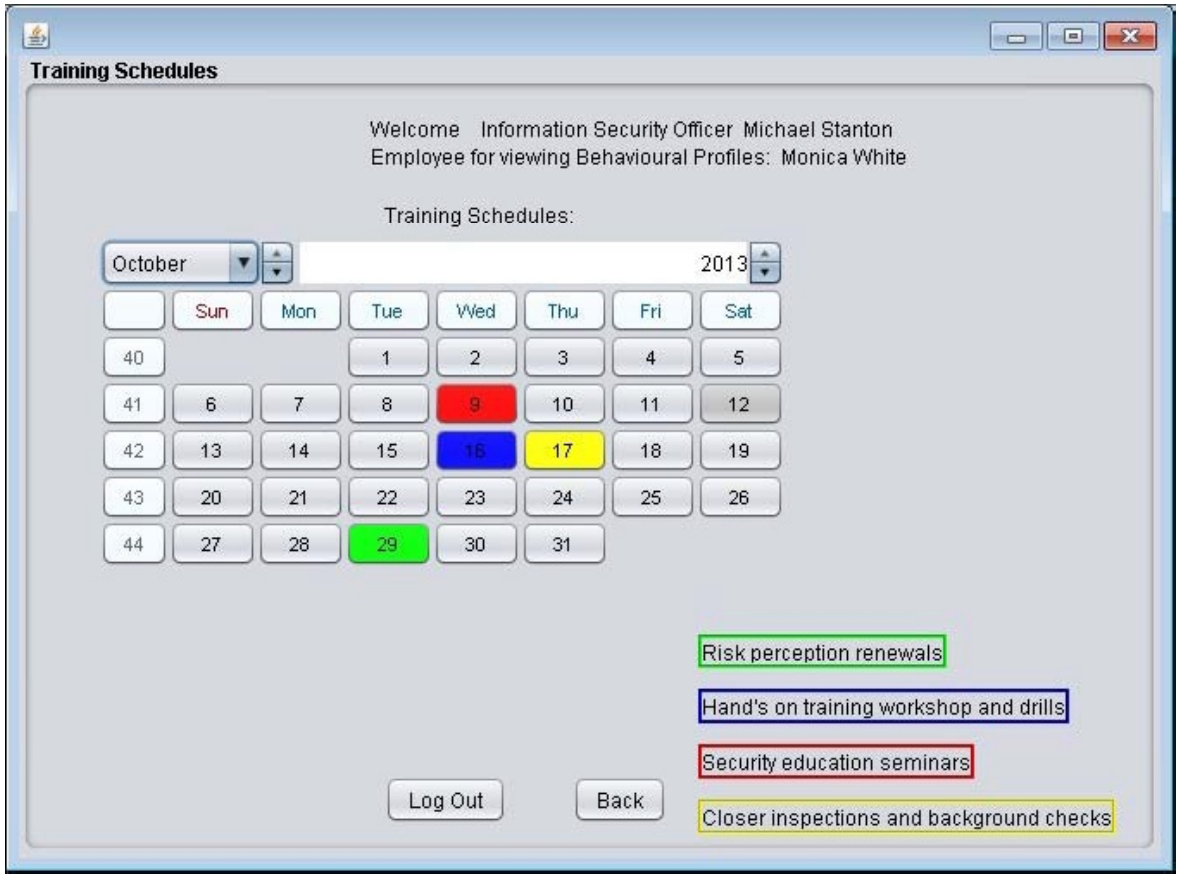

Figure A.10 – Security training schedules for Monica White (Emp0002)

Figure A.11 – Summarized behavioural profile of Shaun Mills (Emp0003)

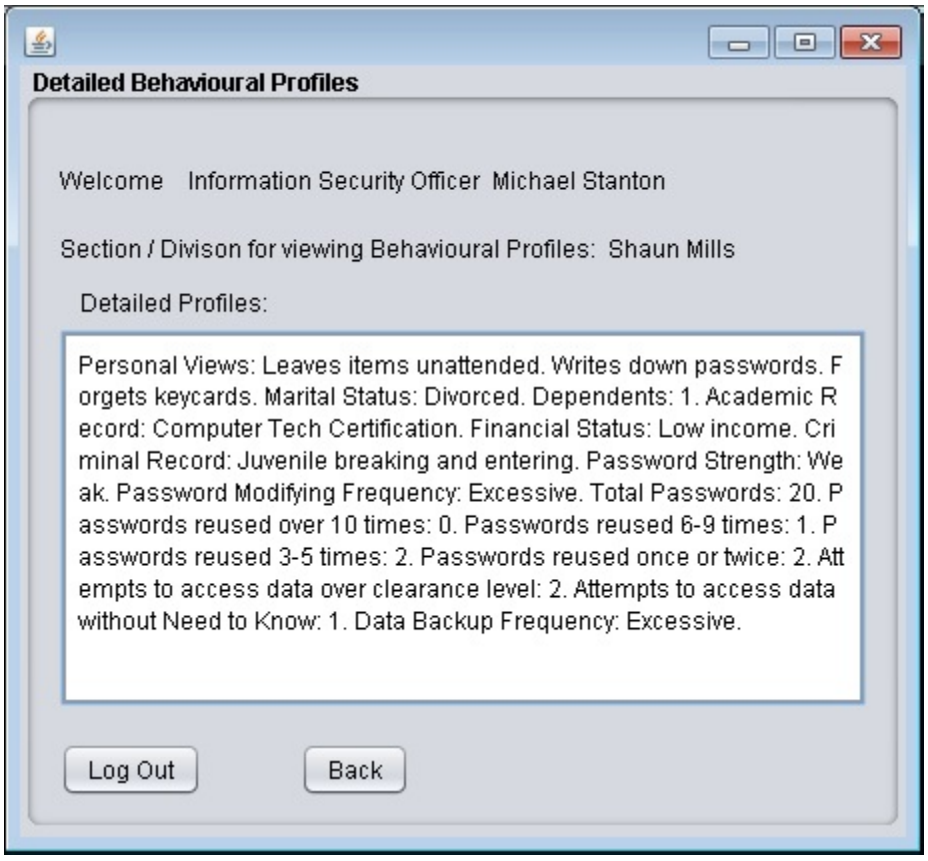

Figure A.12 – Detailed behavioural profile of Shaun Mills (Emp0003)

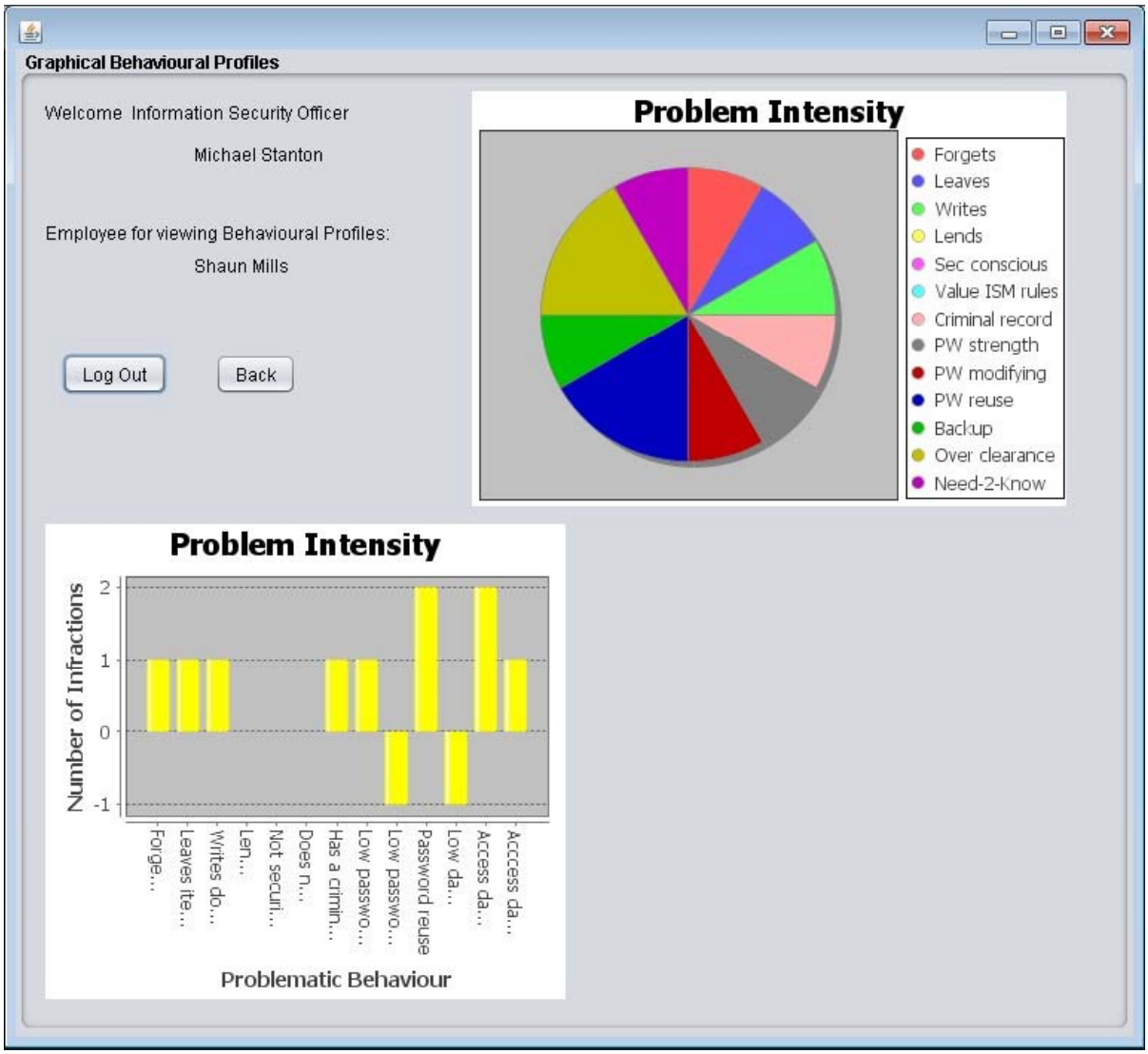

Figure A.13 – Graphical behavioural profile of Shaun Mills (Emp0003)

Figure A.14 – Separate views of the behavioural profile of Shaun Mills (Emp0003)

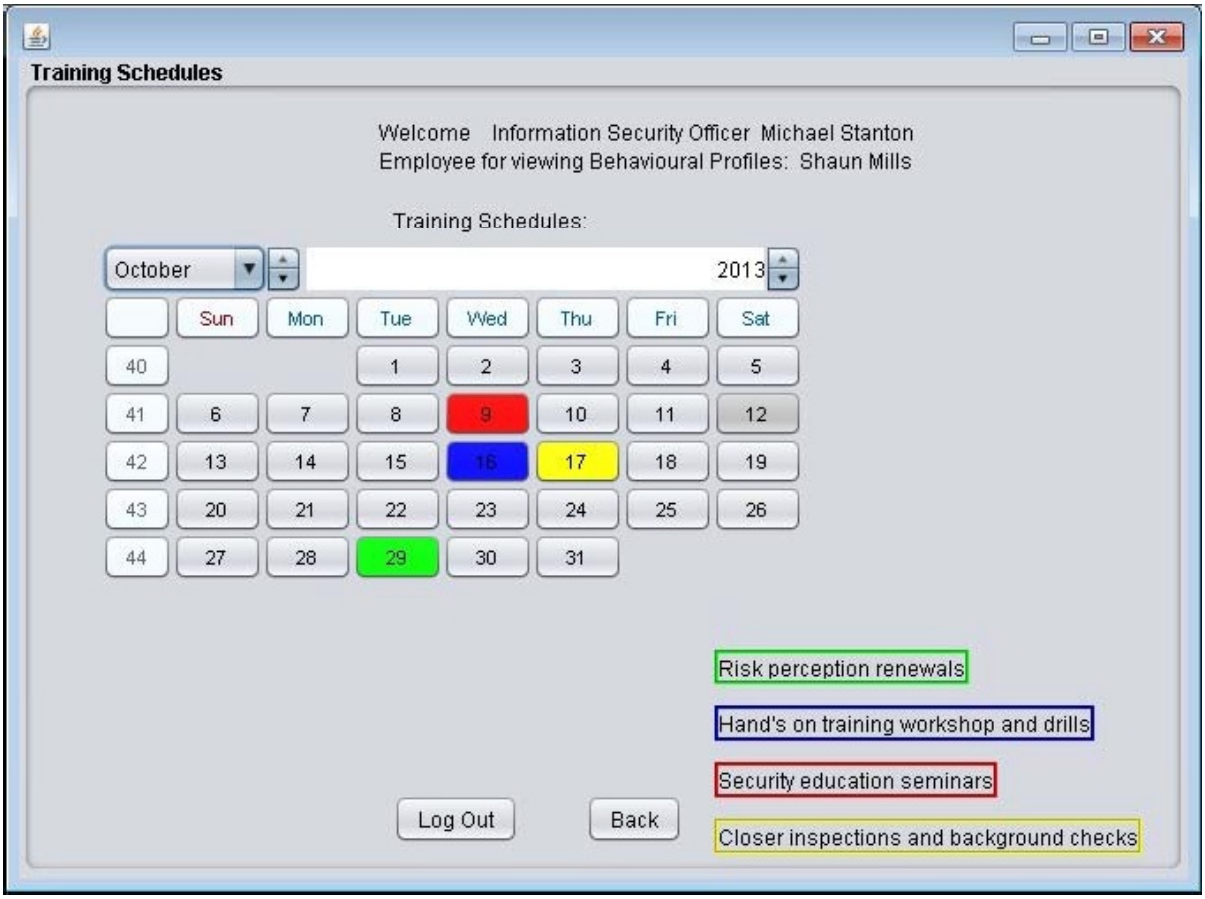

Figure A.15 – Security training schedules for Shaun Mills (Emp0003)

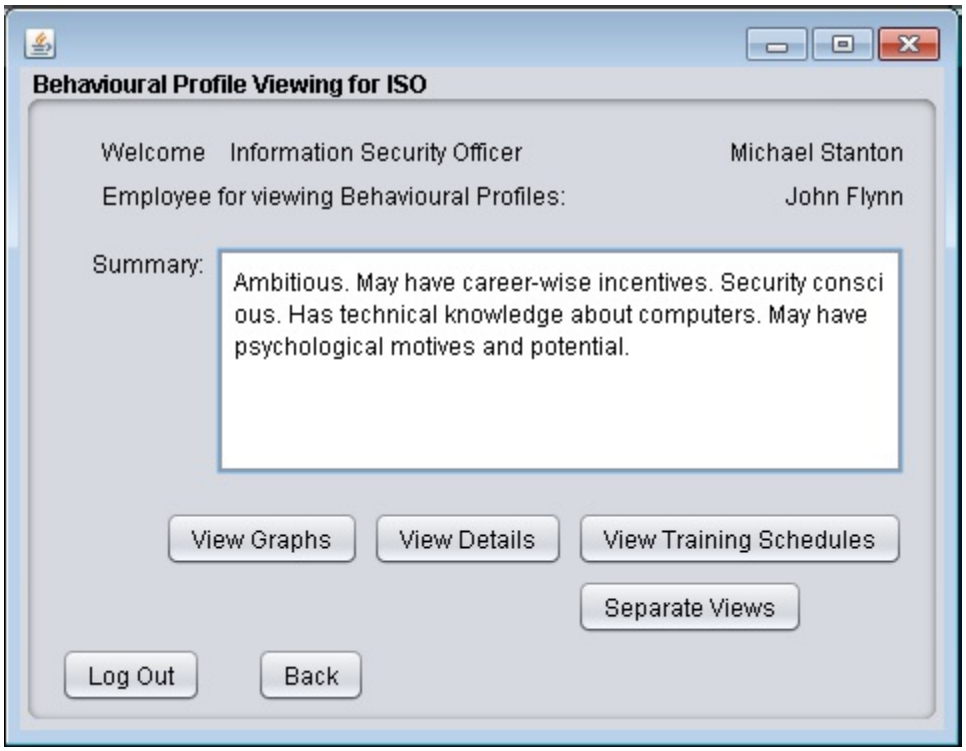

Figure A.16 – Summarized behavioural profile of John Flynn (Emp0004)

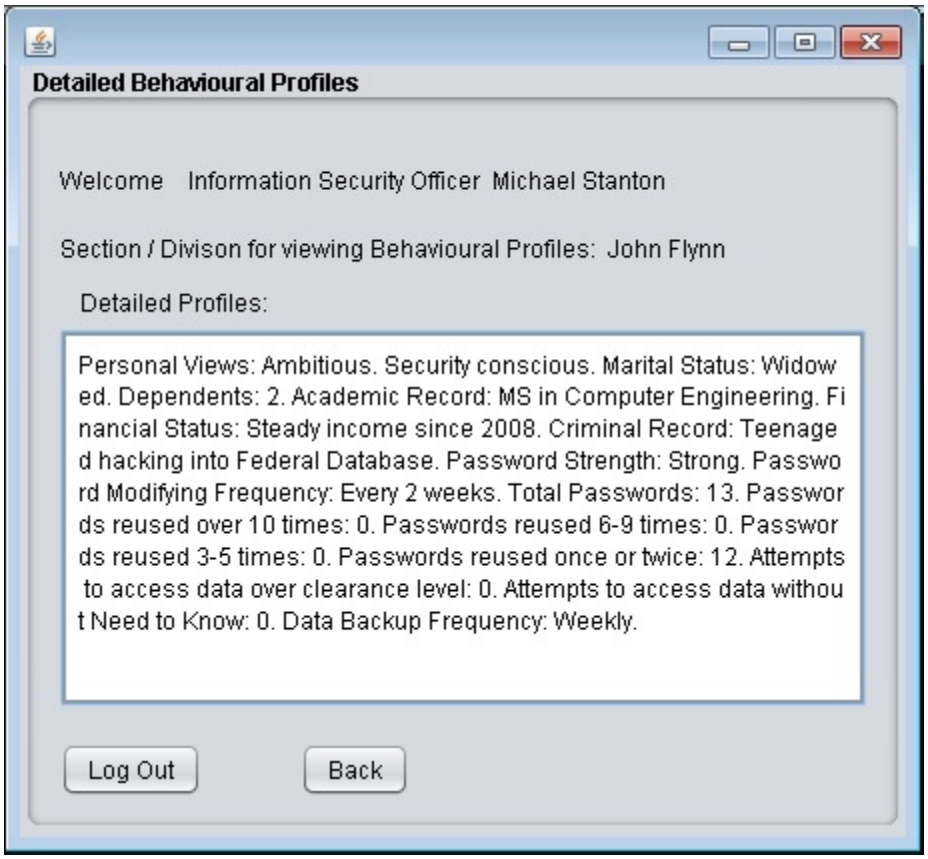

Figure A.17 – Detailed behavioural profile of John Flynn (Emp0004)

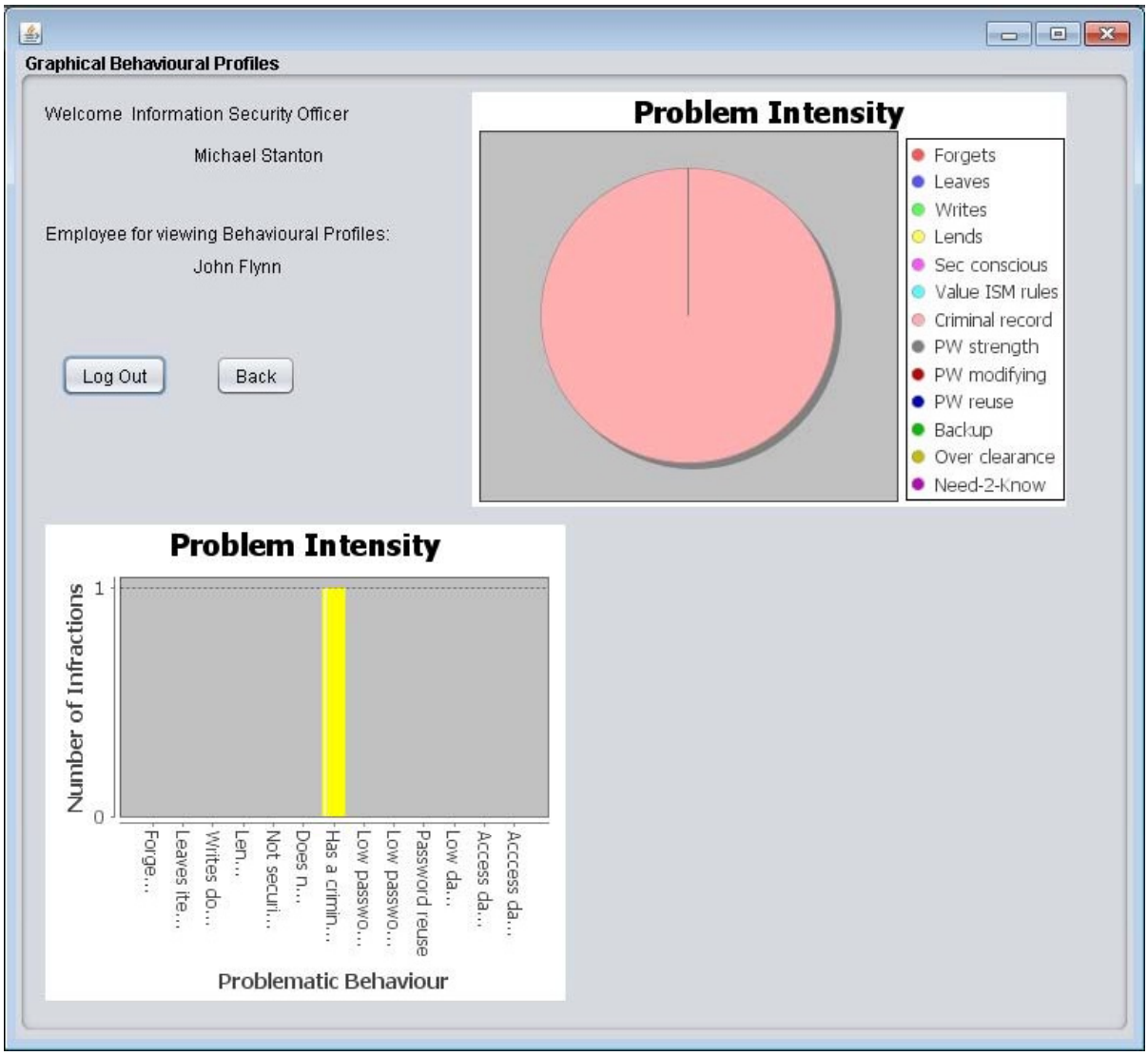

Figure A.18 – Graphical behavioural profile of John Flynn (Emp0004)

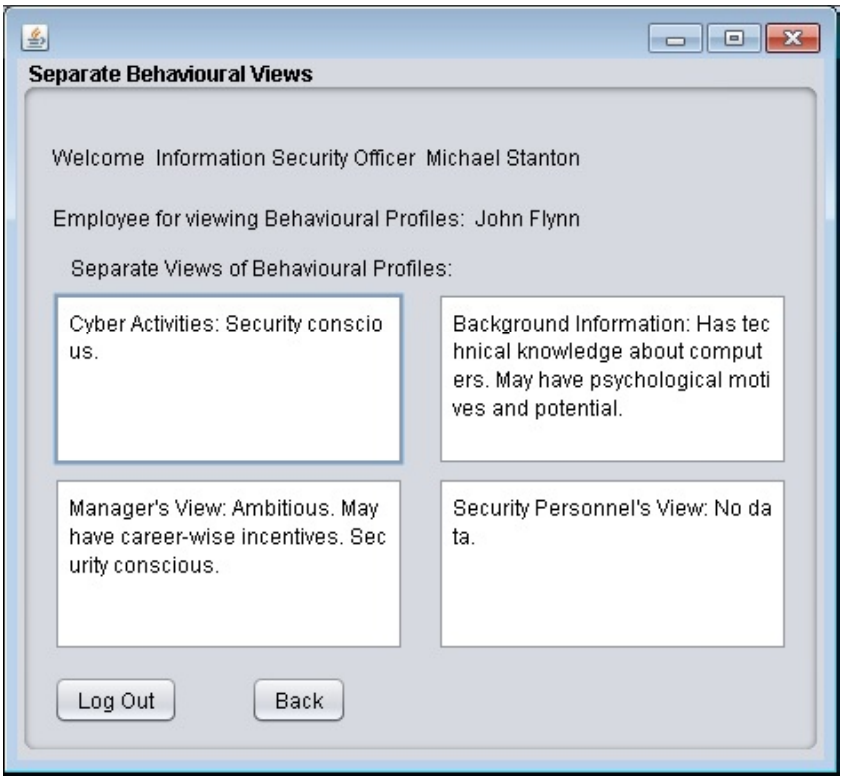

Figure A.19 – Separate views of the behavioural profile of John Flynn (Emp0004)

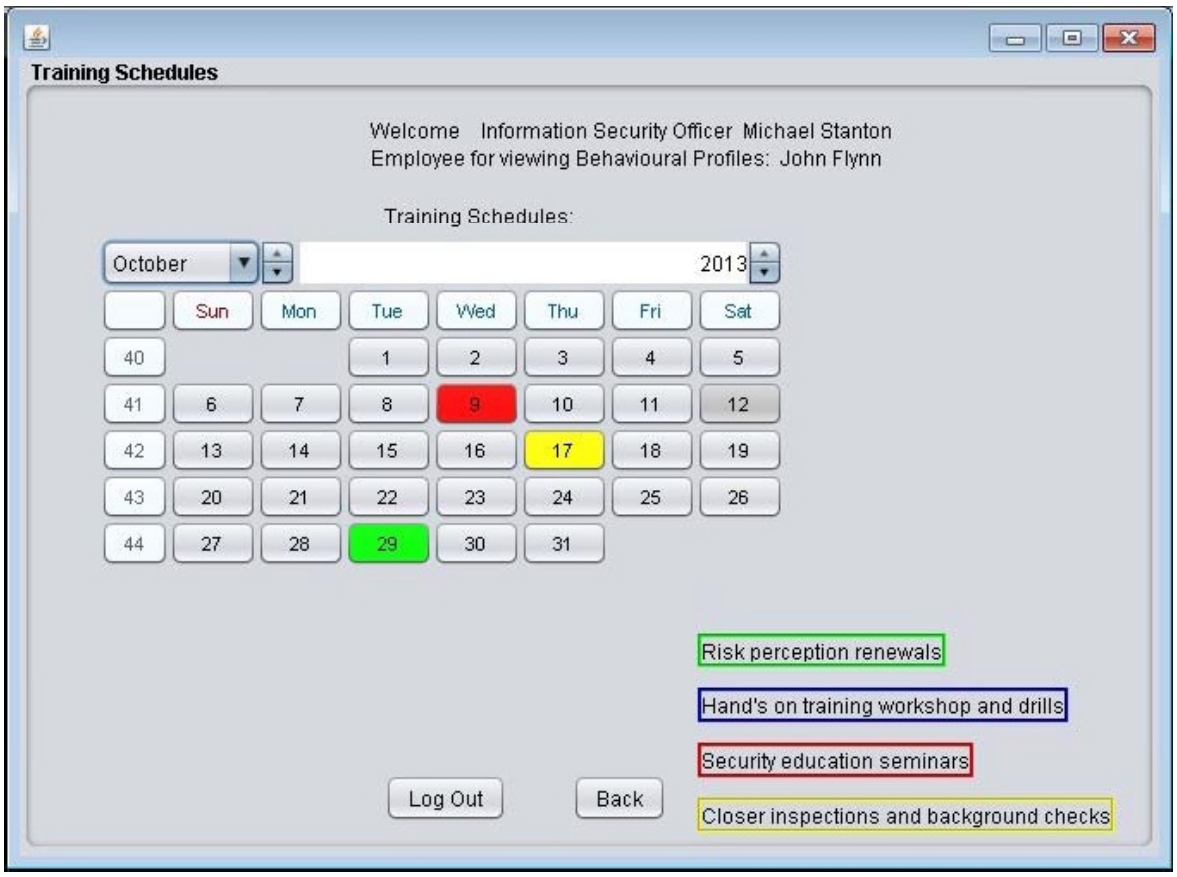

Figure A.20 – Security training schedules for John Flynn (Emp0004)

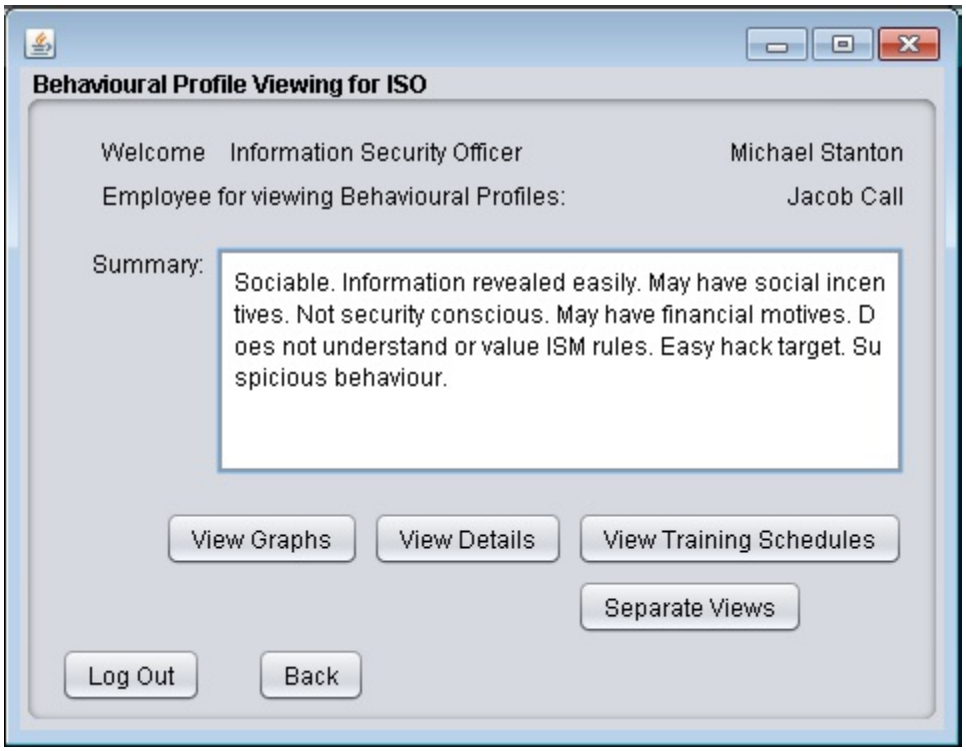

Figure A.21 – Summarized behavioural profile of Jacob Call (Emp0005)

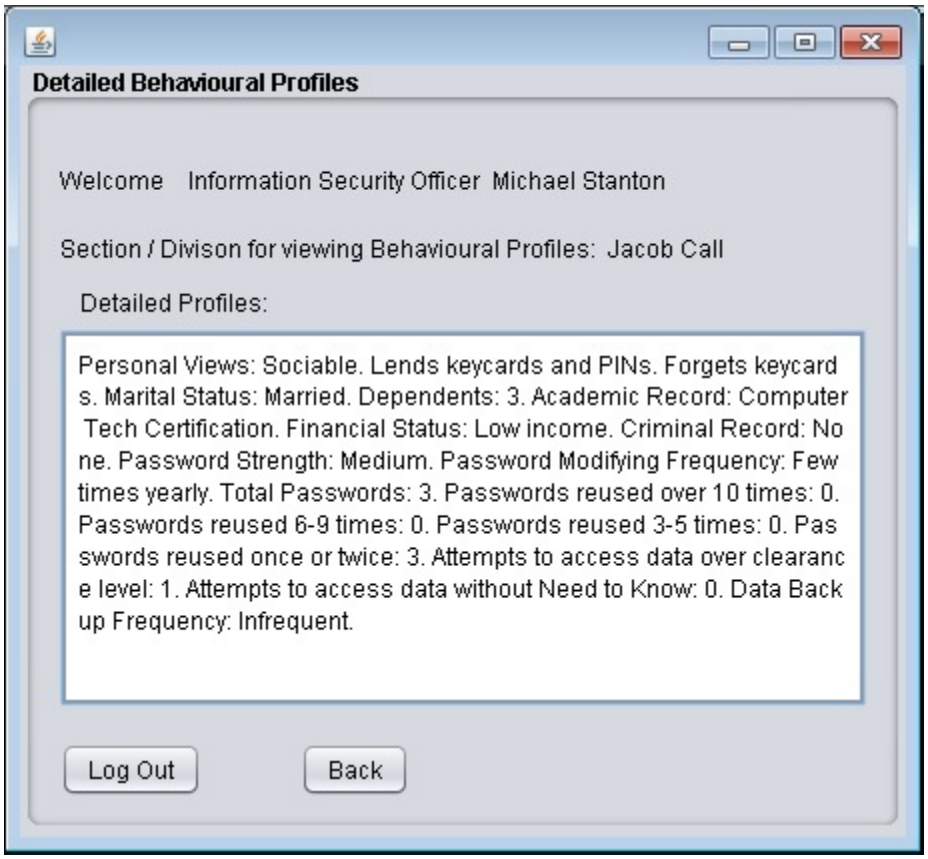

Figure A.22 – Detailed behavioural profile of Jacob Call (Emp0005)

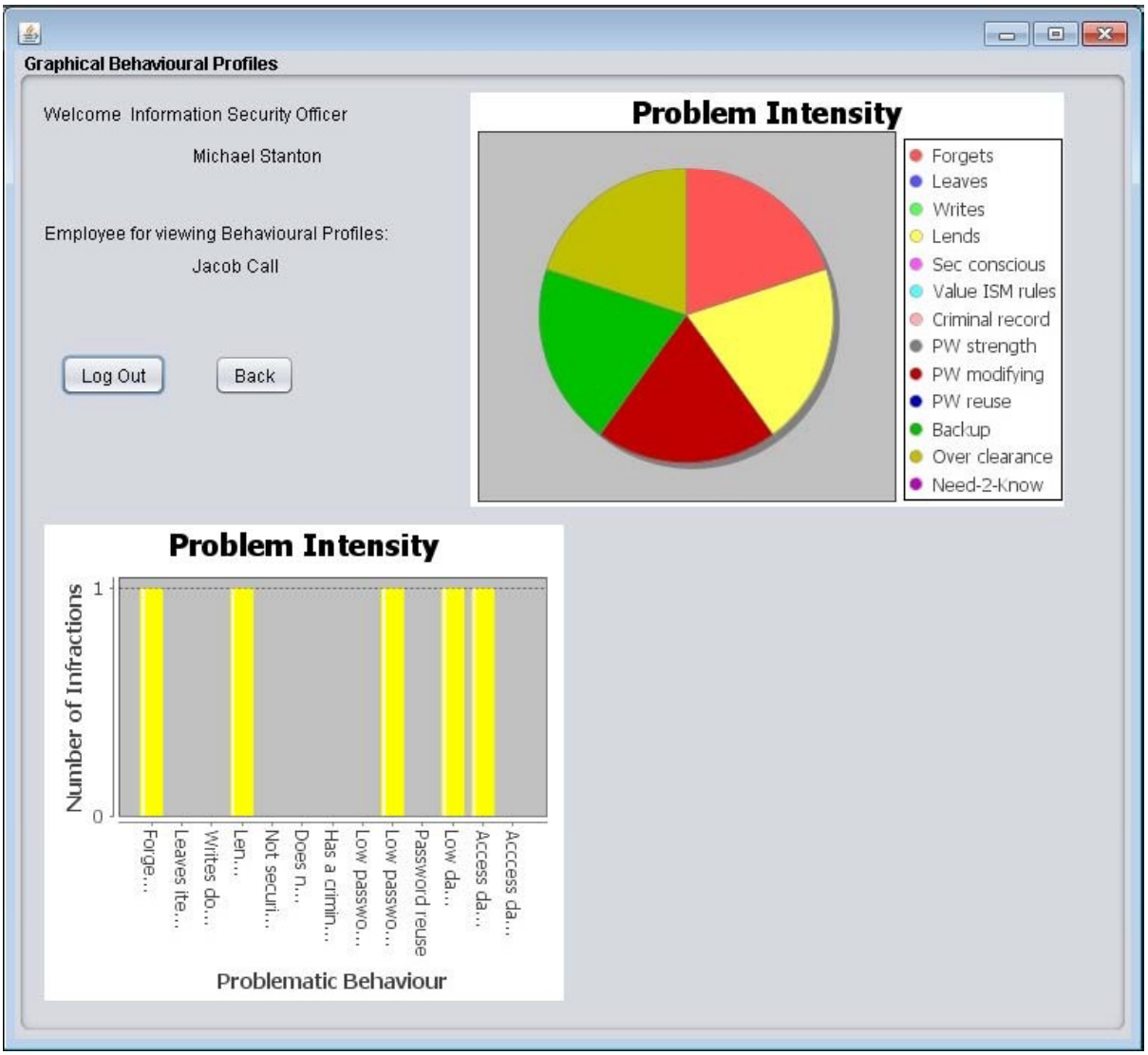

Figure A.23 – Graphical behavioural profile of Jacob Call (Emp0005)

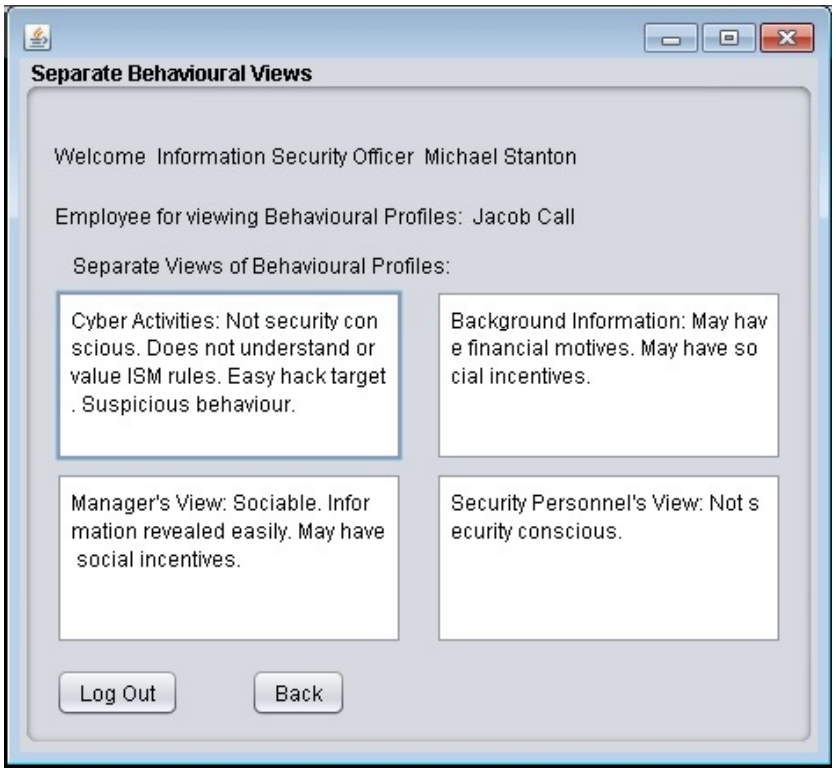

Figure A.24 – Separate views of the behavioural profile of Jacob Call (Emp0005)

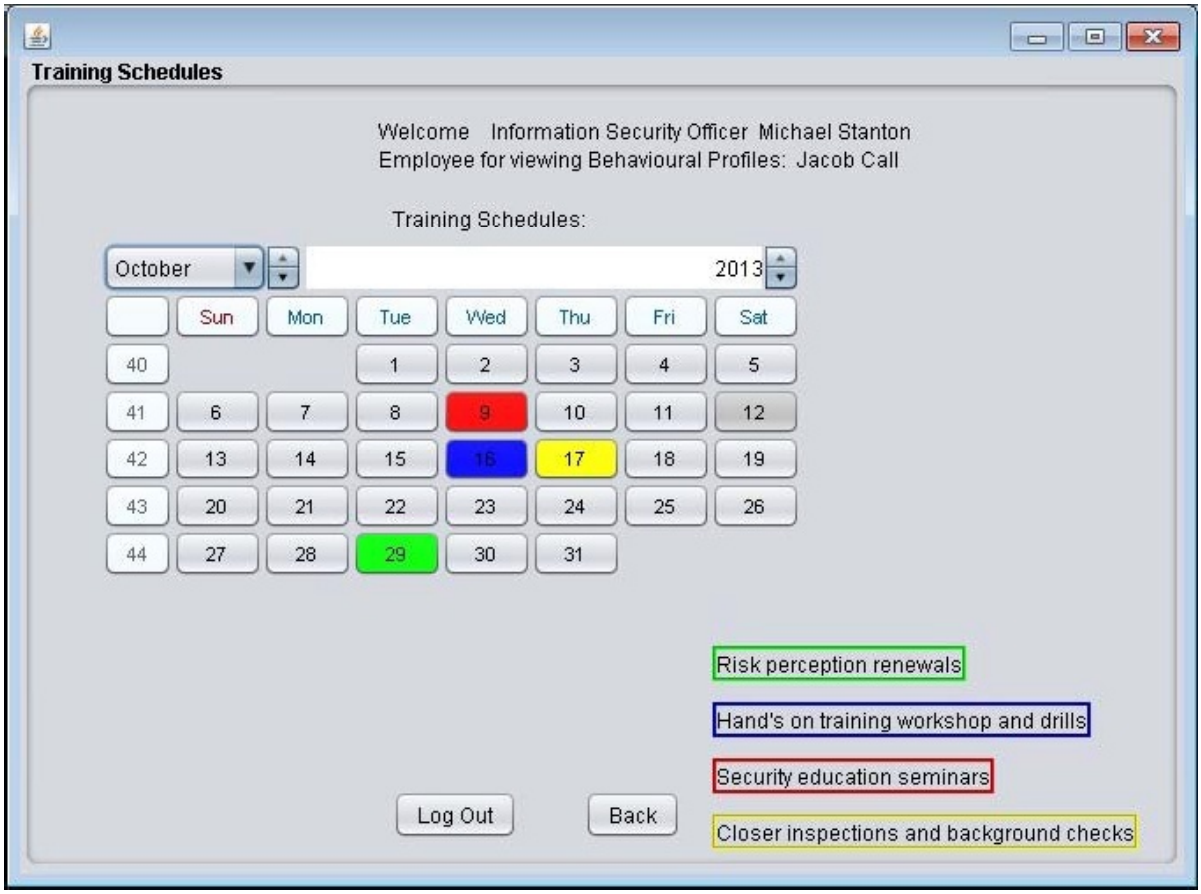

Figure A.25 – Security training schedules for Jacob Call (Emp0005)

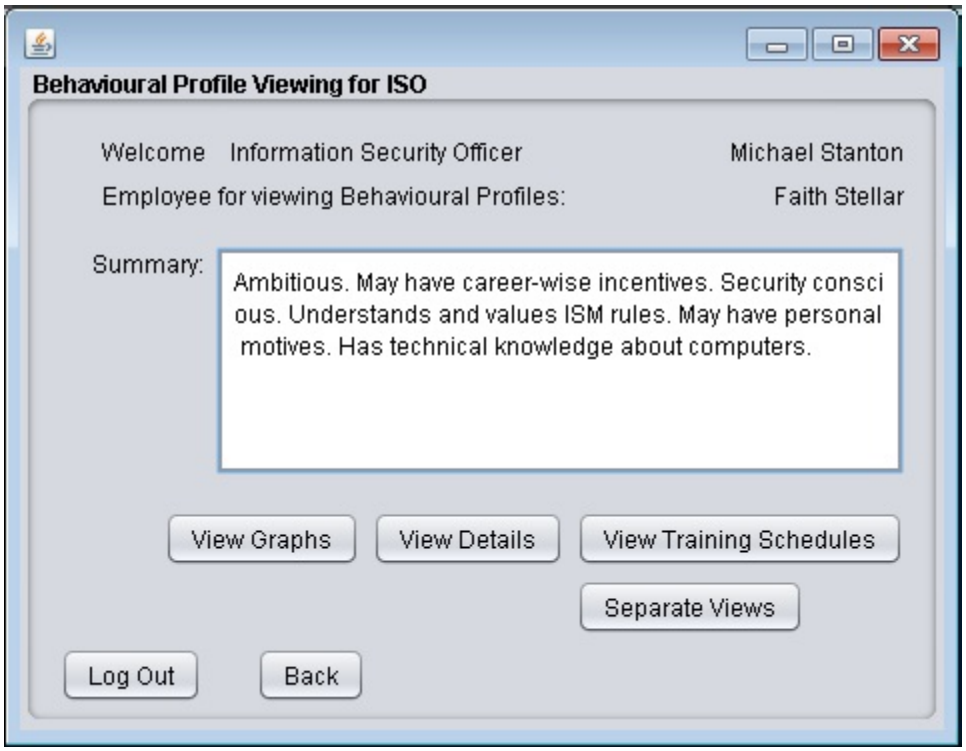

Figure A.26 – Summarized behavioural profile of Faith Stellar (Emp0006)

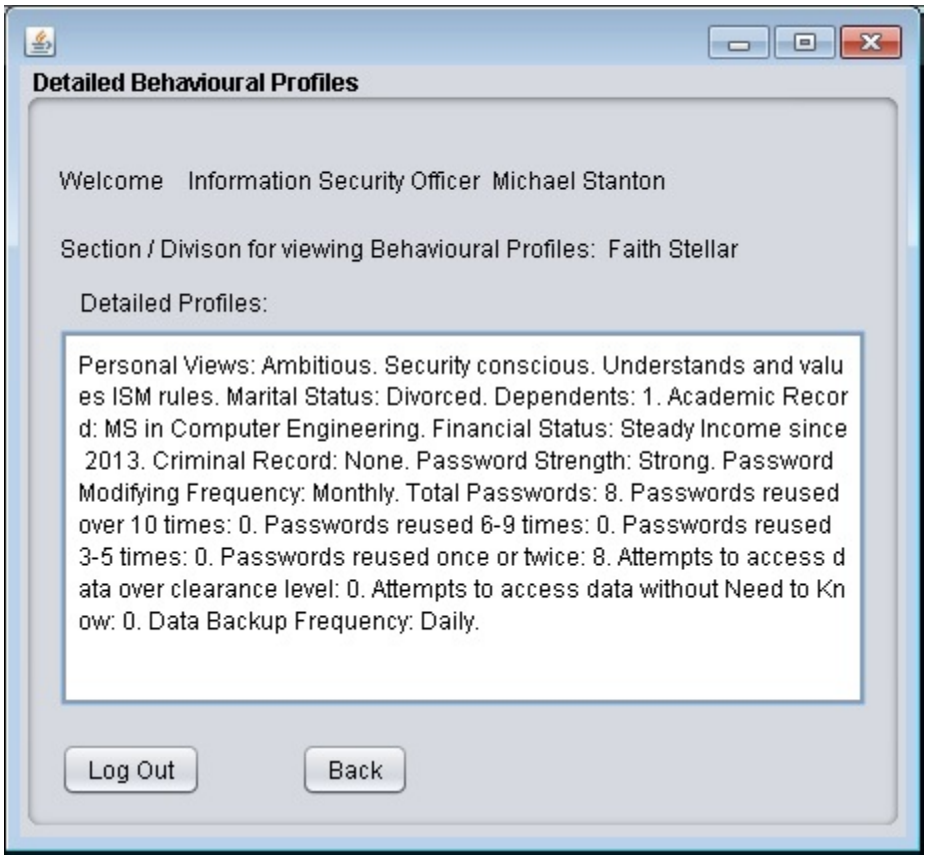

Figure A.27 – Detailed behavioural profile of Faith Stellar (Emp0006)

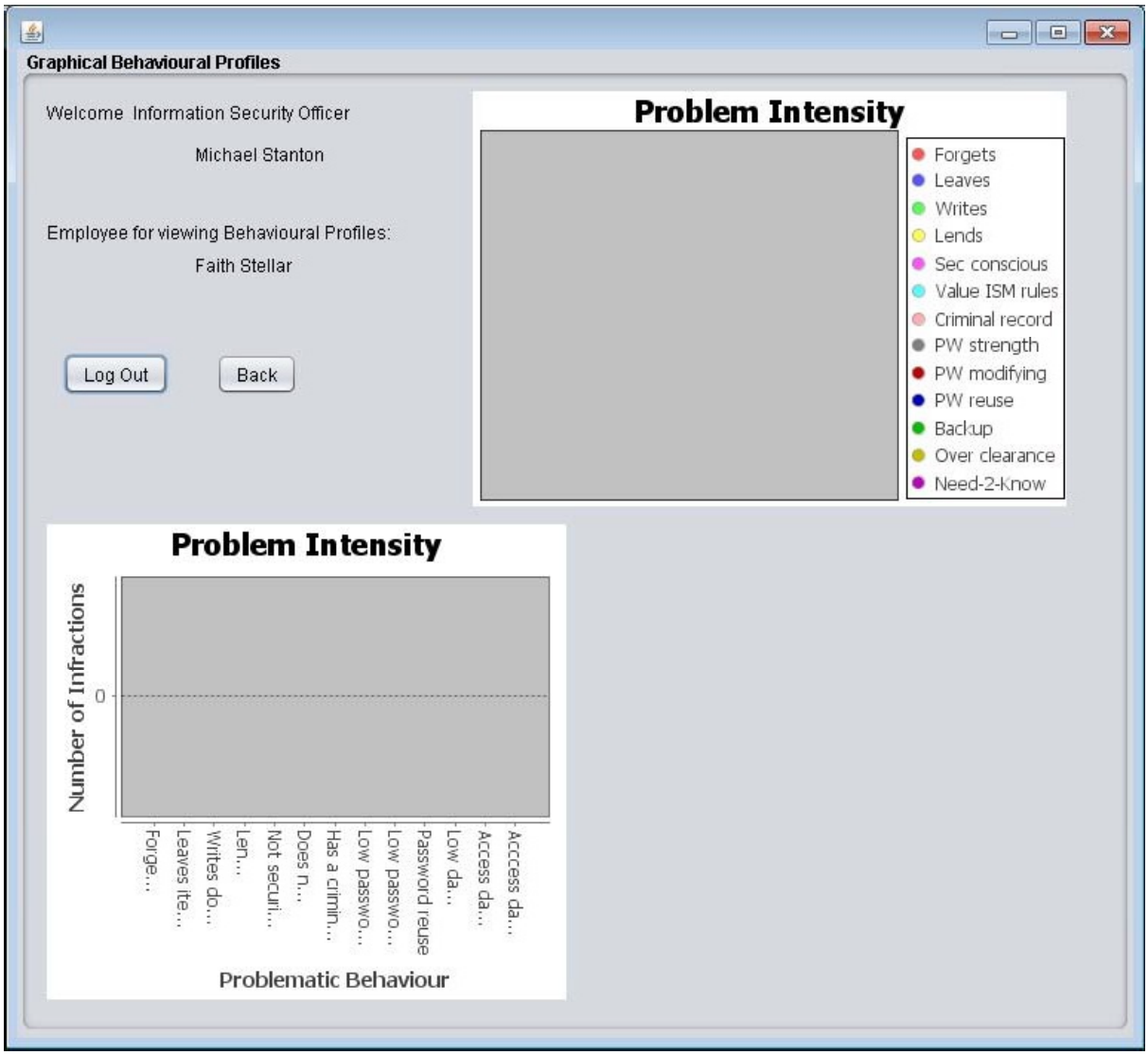

Figure A.28 – Graphical behavioural profile of Faith Stellar (Emp0006)

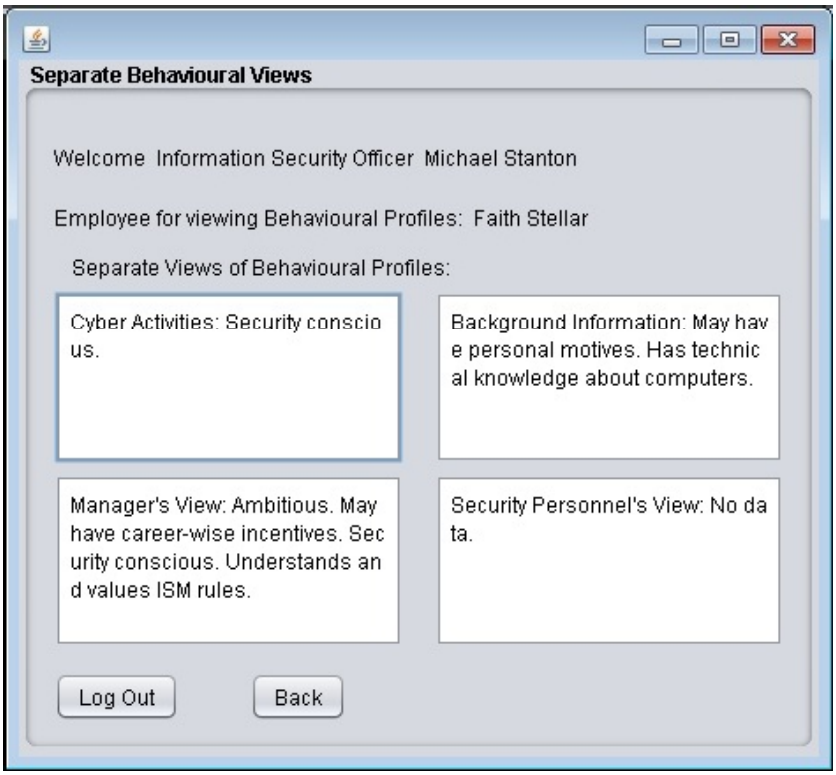

Figure A.29 – Separate views of the behavioural profile of Faith Stellar (Emp0006)

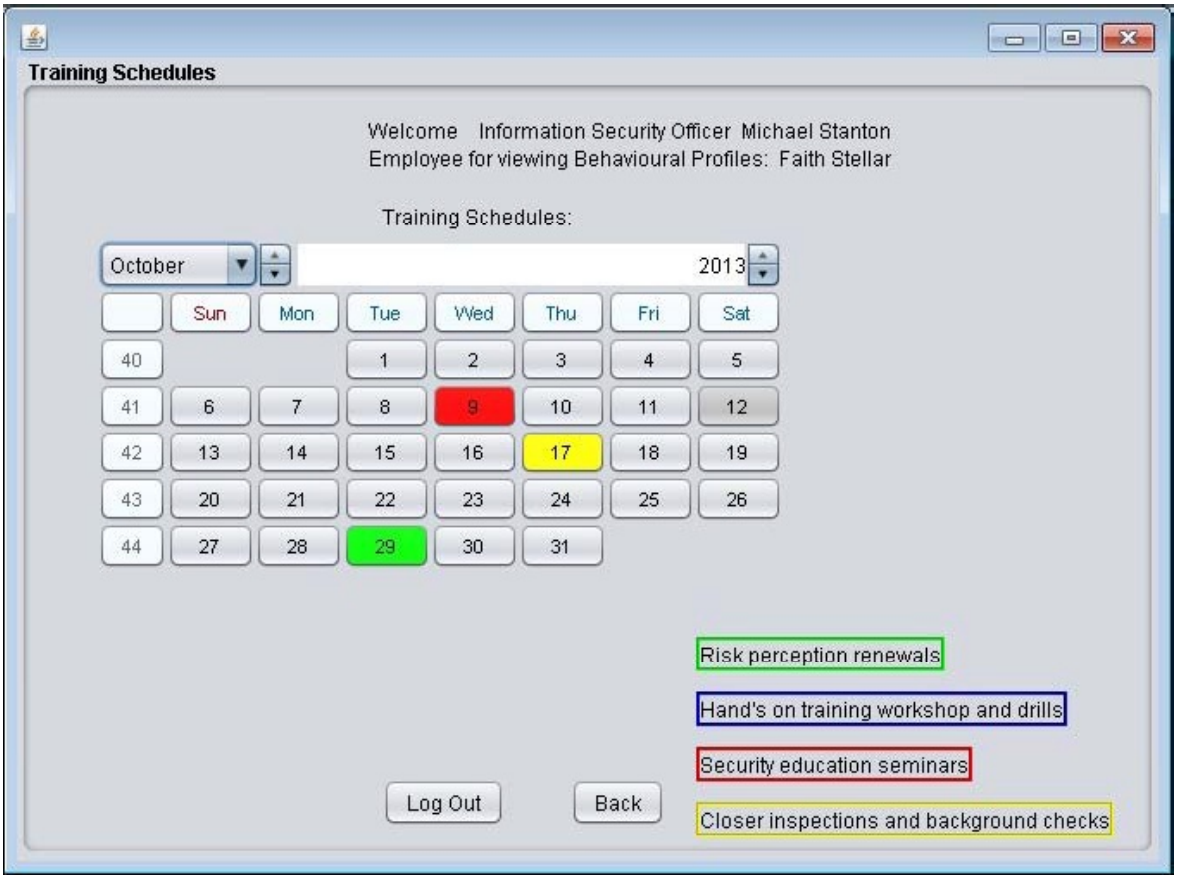

Figure A.30 – Security training schedules for Faith Stellar (Emp0006)

Figure A.31 – Summarized behavioural profile of Clair McCormick (Emp0007)

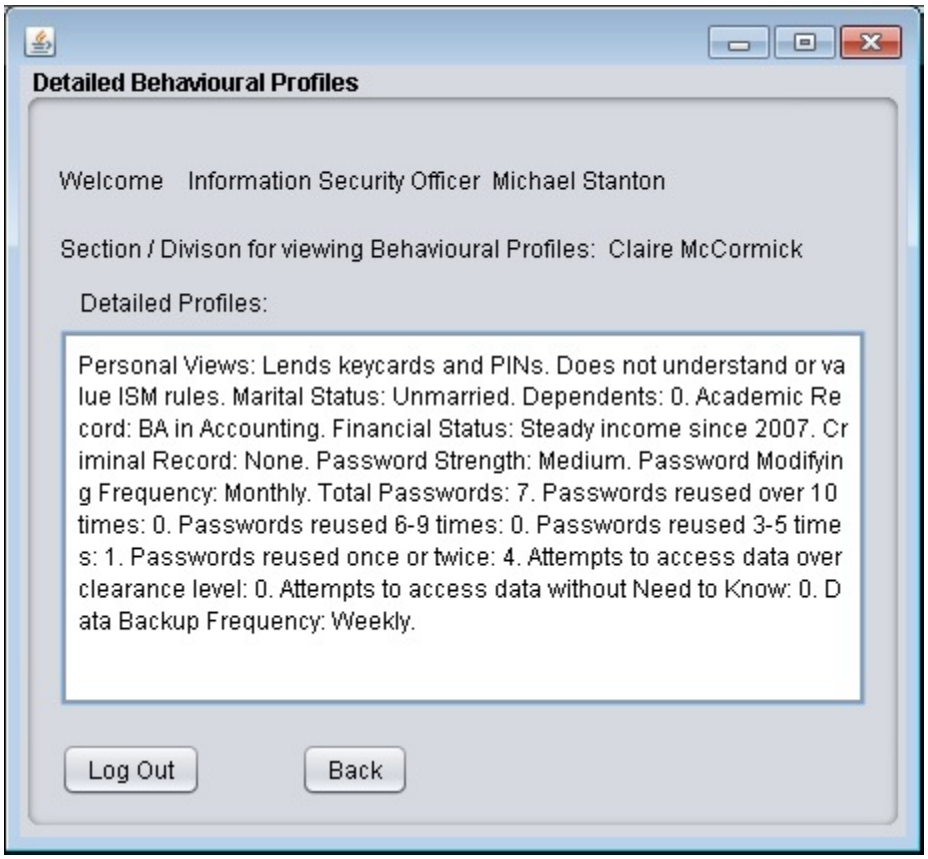

Figure A.32 – Detailed behavioural profile of Clair McCormick (Emp0007)

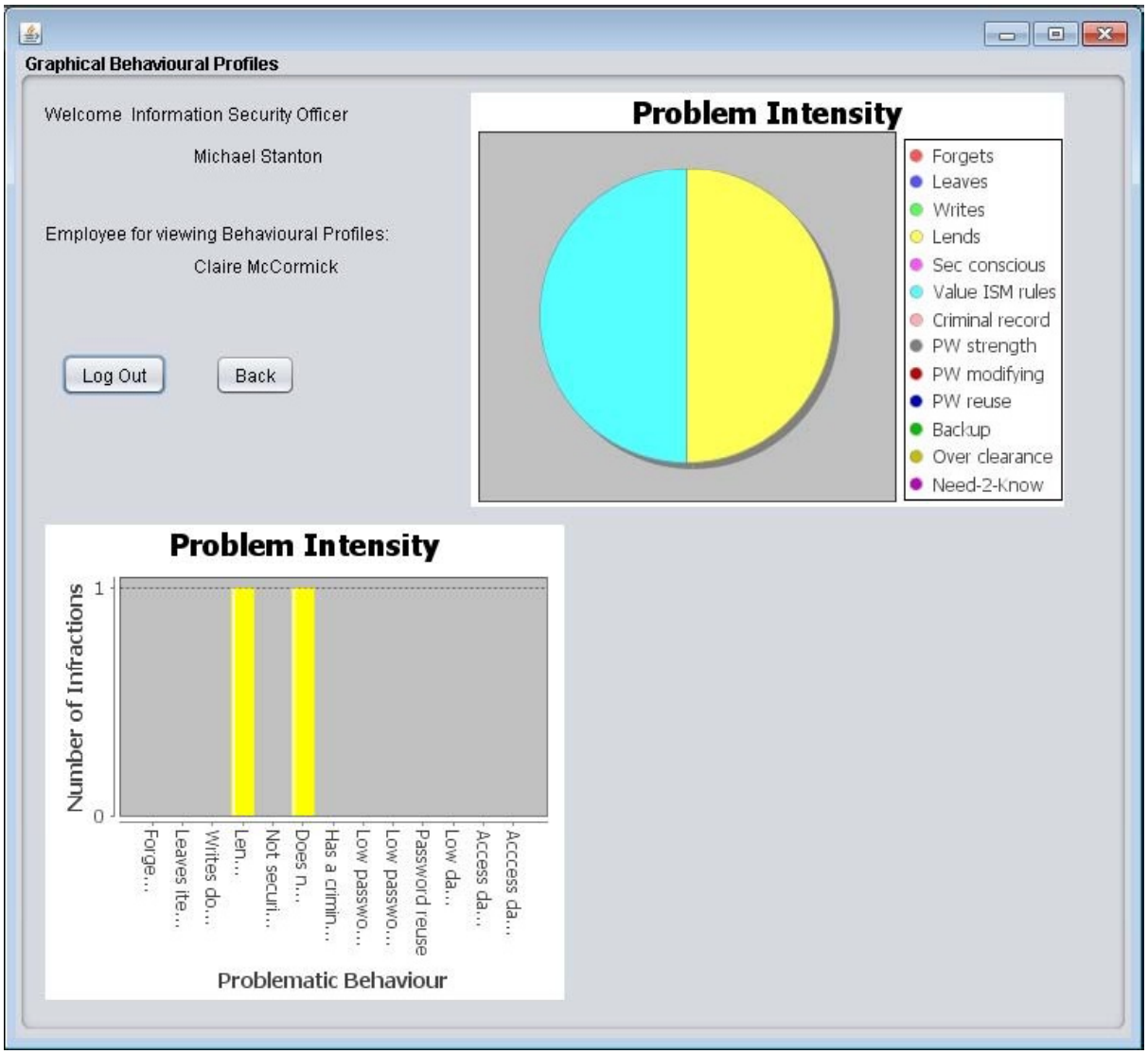

Figure A.33 – Graphical behavioural profile of Clair McCormick (Emp0007)

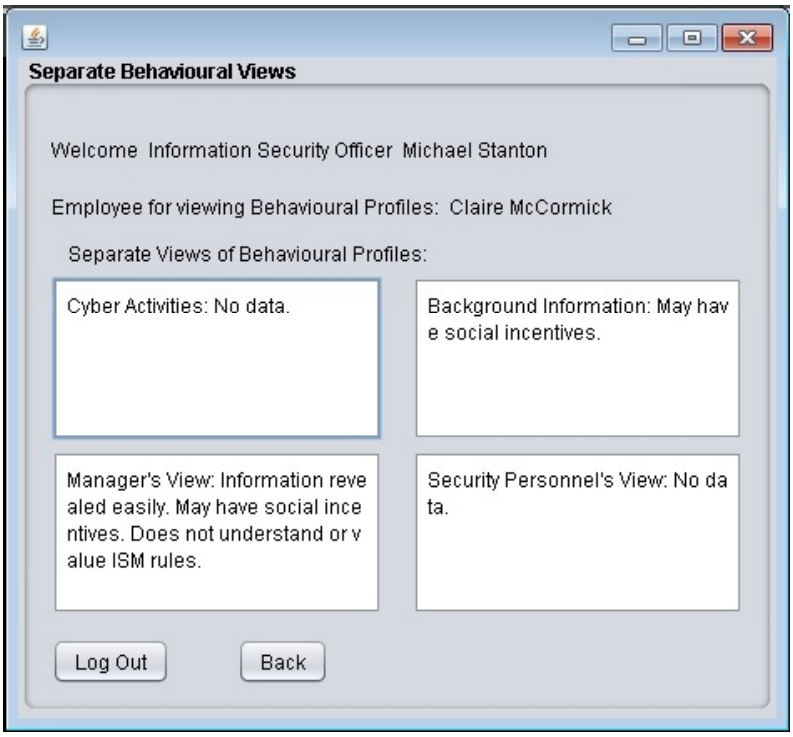

Figure A.34 – Separate views of the behavioural profile of Clair McCormick (Emp0007)

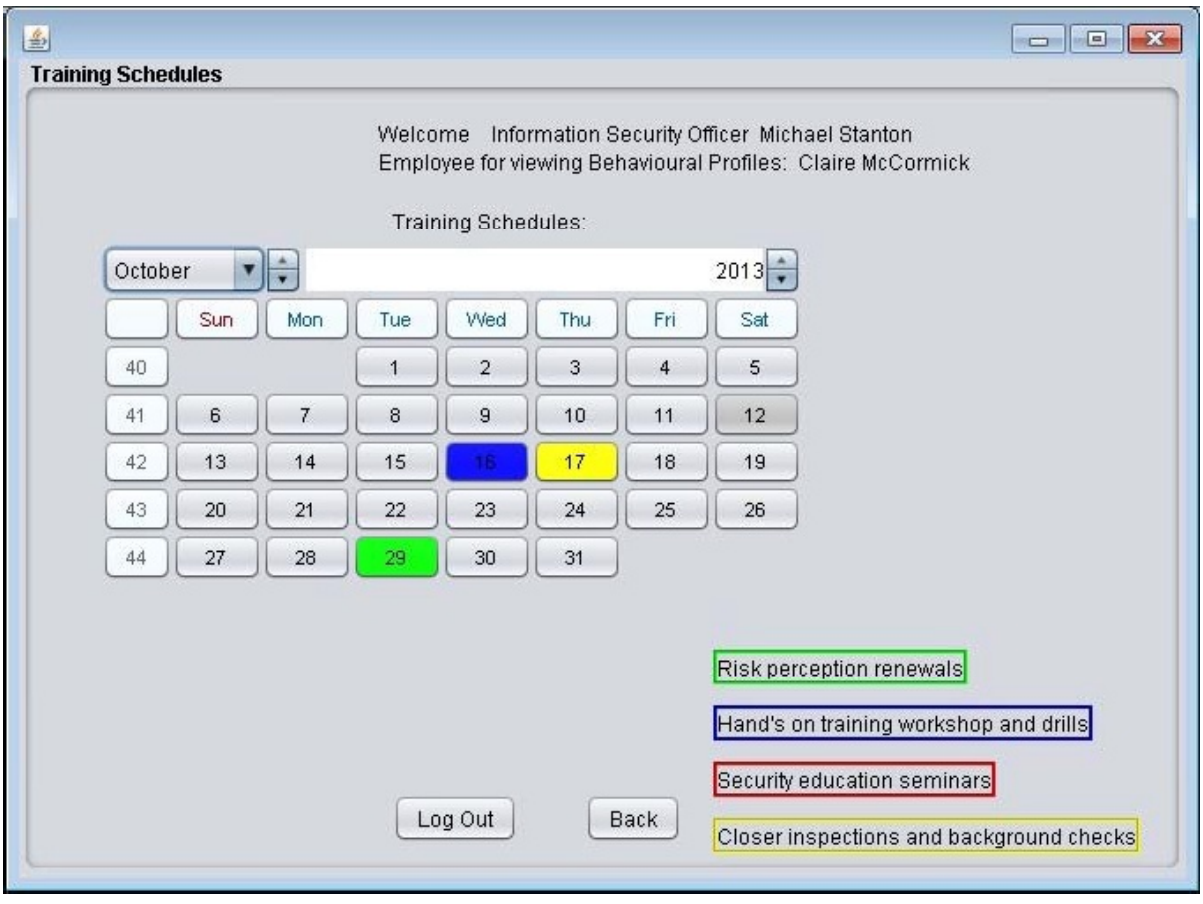

Figure A.35 – Security training schedules for Clair McCormick (Emp0007)

Figure A.36 – Summarized behavioural profile of Gavin Fields (Emp0009)

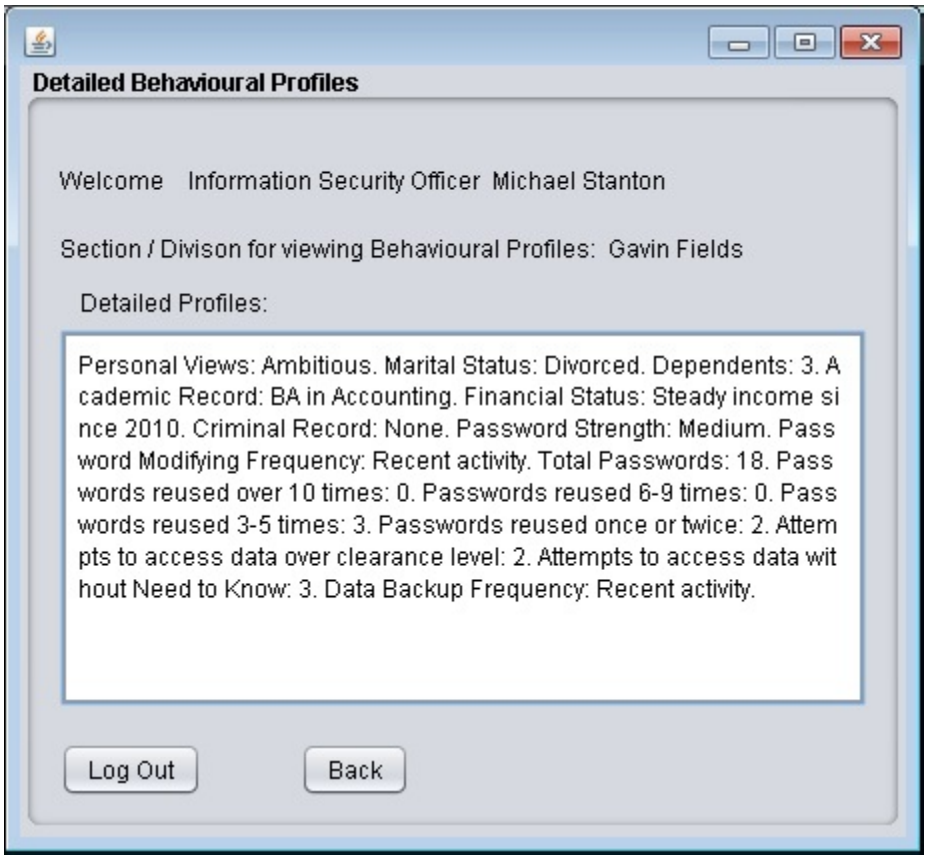

Figure A.37 – Detailed behavioural profile of Gavin Fields (Emp0009)

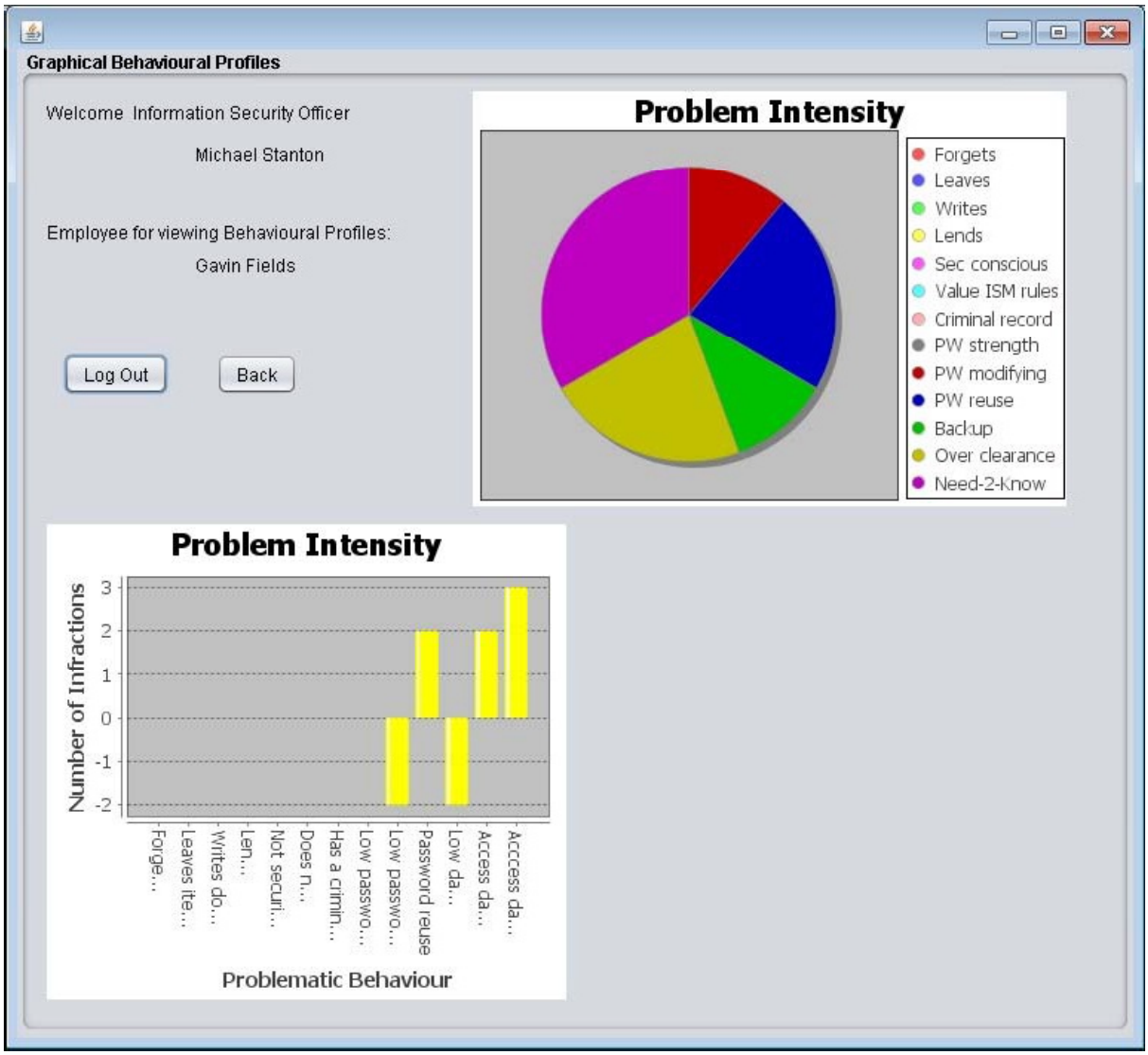

Figure A.38 – Graphical behavioural profile of Gavin Fields (Emp0009)

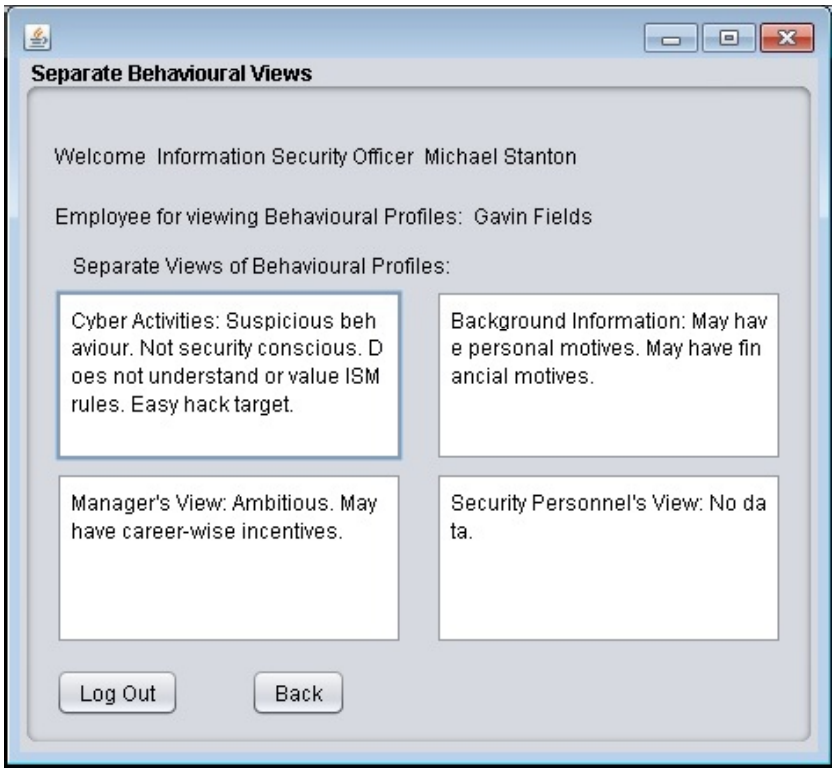

Figure A.39 – Separate views of the behavioural profile of Gavin Fields (Emp0009)

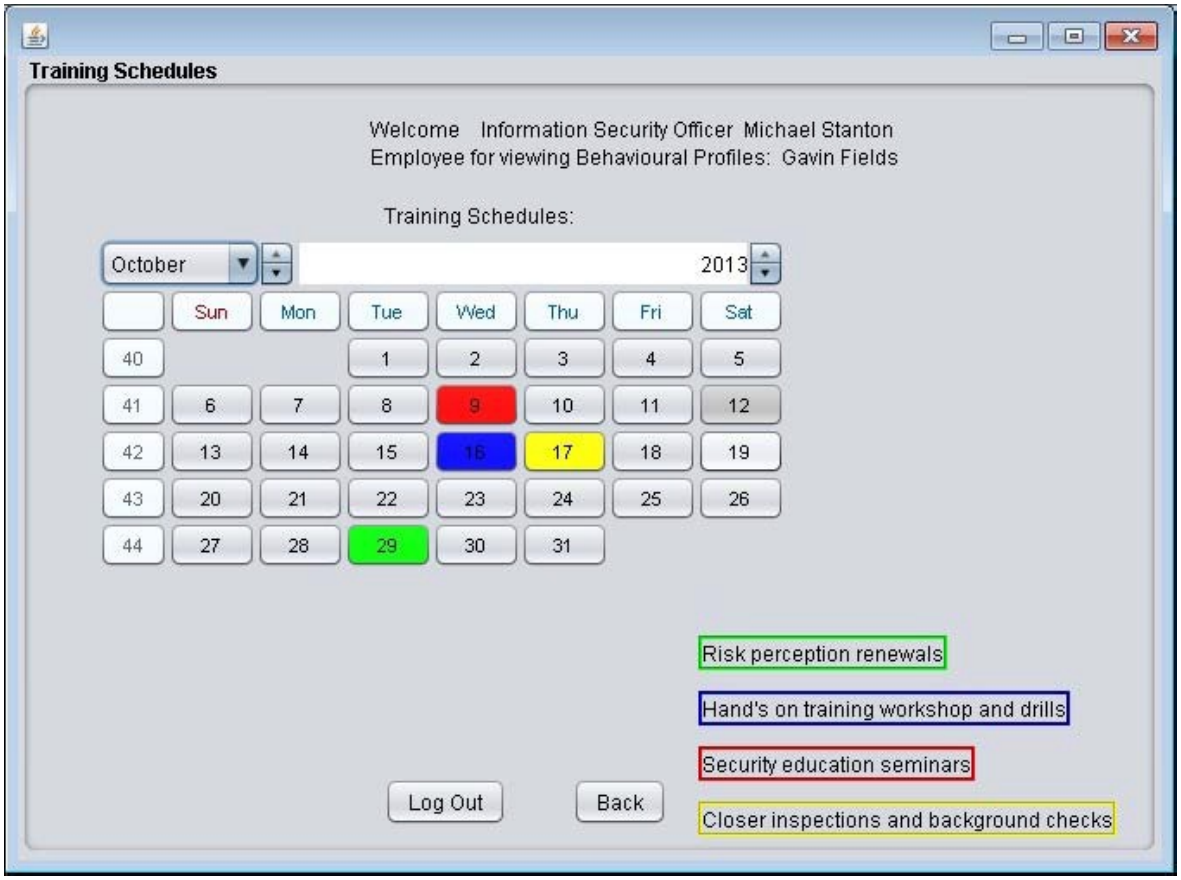

Figure A.40 – Security training schedules for Gavin Fields (Emp0009)

Figure A.41 – Summarized behavioural profile of Sarah Mason (Emp0010)

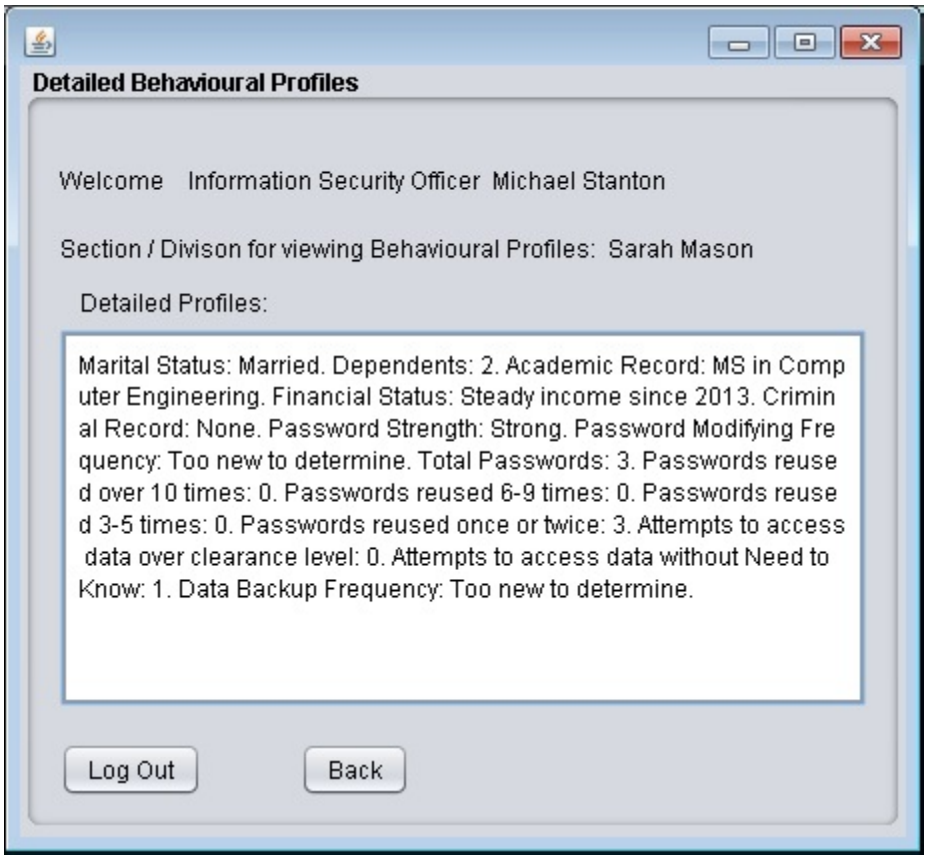

Figure A.42 – Detailed behavioural profile of Sarah Mason (Emp0010)

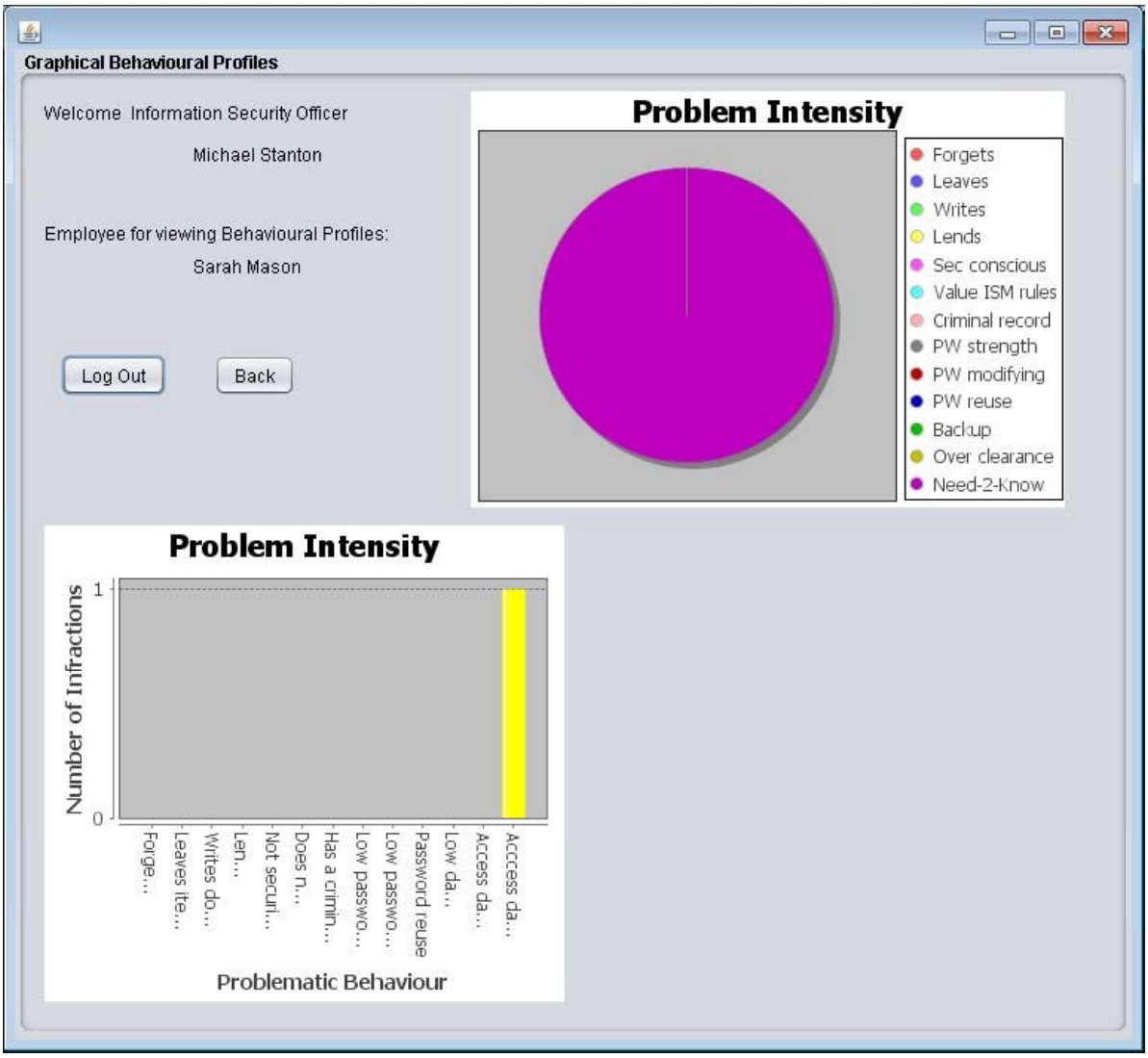

Figure A.43 – Graphical behavioural profile of Sarah Mason (Emp0010)

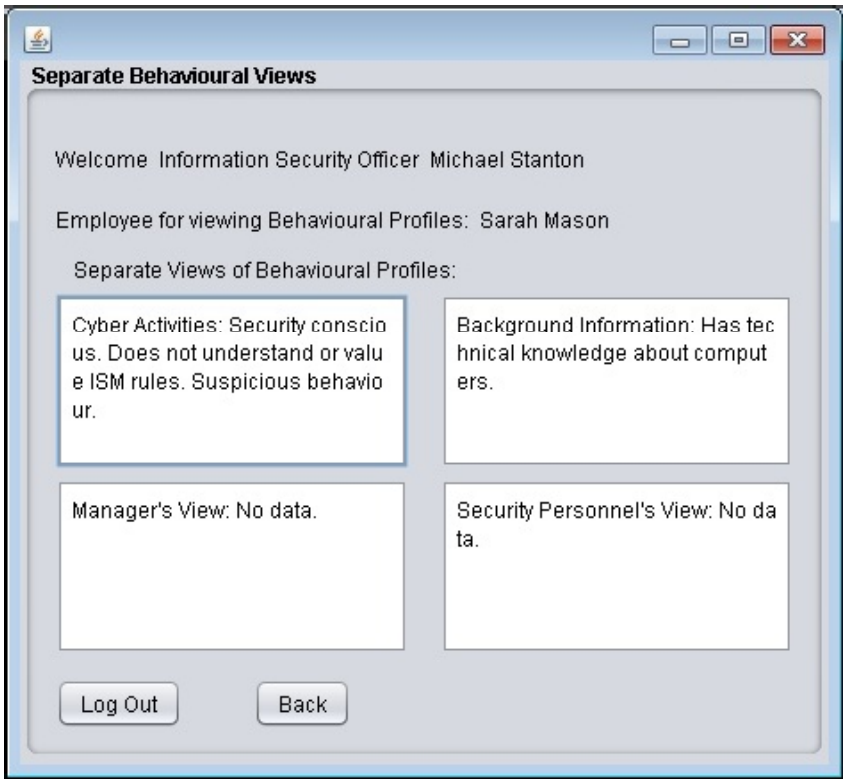

Figure A.44 – Separate views of the behavioural profile of Sarah Mason (Emp0010)

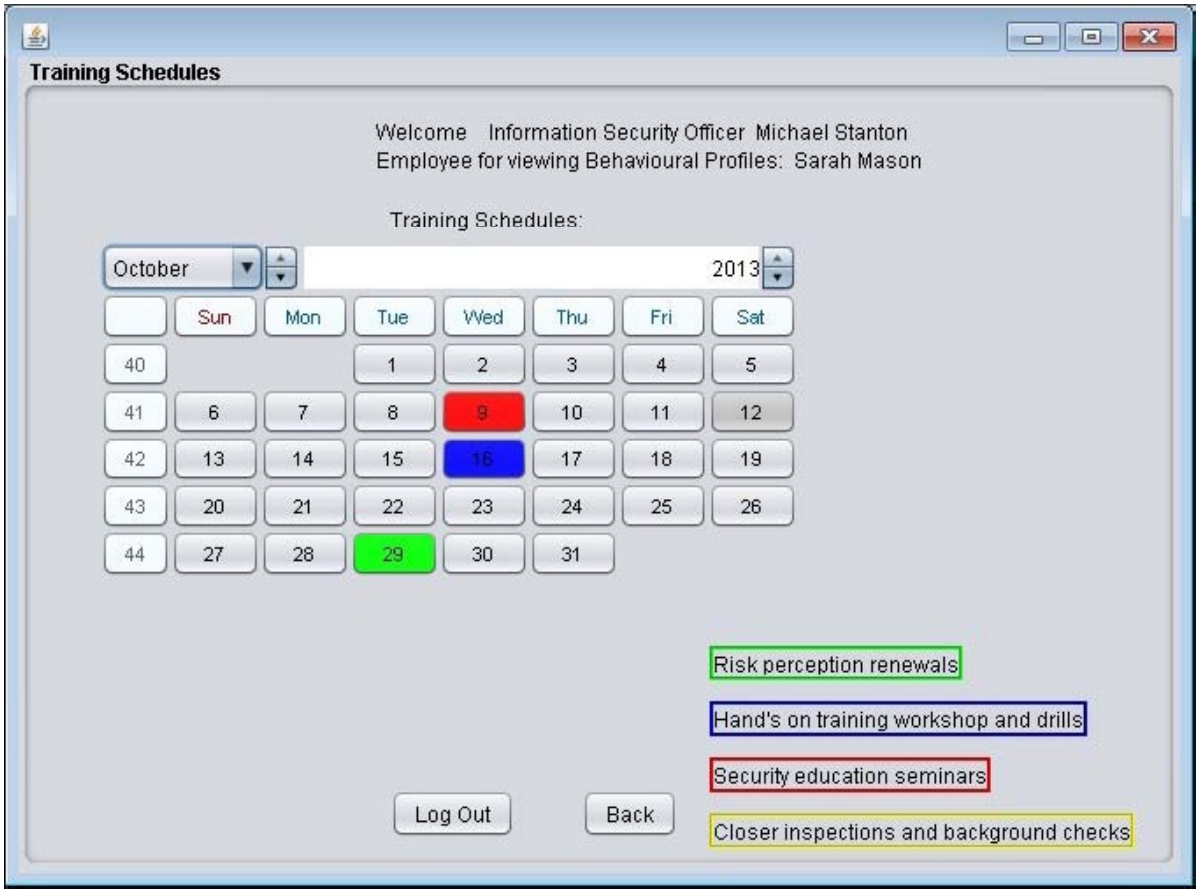

Figure A.45 – Security training schedules for Sarah Mason (Emp0010)

Appendix B – Algorithms

Table B.1 – Complete Algorithm for Determining Password Modifying Frequency

Algorithm

```
Start
    modFreq
    yearly count = count pw changes within last 1 year
    total pw = count all pw changes since joining organization
        if (total pw <= yearly count)                                   //Joined less than 1 year ago
            ten month count = count pw changes within last 10 months
            if (total pw <= ten month count)                            //Joined less than 10 months ago
                eight month count = count pw changes within last 8 months
                if (total pw <= eight month count)                      //Joined less than 8 months ago
                    six month count = count pw changes within last 6 months
                    if (total pw <= six month count)                    //Joined less than 6 months ago
                        four month count = count pw changes within last 4 months
                        if (total pw <= four month count)               //Joined less than 4 months ago
                            two month count = count pw changes within last 2 months
                            if (total pw <= two month count)            //Joined less than 2 months ago
                                monthly count = count pw changes within last 1 month
                                if (total pw <= monthly count)          //Joined less than 1 month ago
                                    modFreq = "Too new to determine"
                                else
                                    if(monthly count > 1)
                                        modFreq = do 1month
                                    else if(monthly count == 1)
                                        modFreq = "Monthly"
                                    else                                //monthly count < 1
                                        modFreq = "Infrequent"
                            else
                                if( two month count > 1)
                                    modFreq = do 2months
                                else if(two month count == 1)
                                    modFreq = "Few times yearly"
                                else                                    //two month count < 1
                                    modFreq = "Infrequent"
                        else
                            if( four month count > 2)
                                modFreq = do 4months
                            else if(four month count == 2)
                                modFreq = "Few times yearly"
                            else                                        //four month count < 2
                                modFreq = "Infrequent"
                    else
                        if( six month count > 2)
                            modFreq = do 6months
                        else if(six month count == 2)
                            modFreq = "Few times yearly"
                        else                                            //six month count < 2
                            modFreq = "Infrequent"
                else
                    if( eight month count > 3)
                        modFreq = do 8months
                    else if(eight month count == 3)
                        modFreq = "Few times yearly"
                    else                                                //eight month count  < 3
                        modFreq = "Infrequent"
            else
                if( ten month count > 3)
                    modFreq = do 10months
                else if(ten month count == 3)
```

Algorithm

```
                        modFreq = “Few times yearly”
                else                                                    //ten month count < 3
                        modFreq = “Infrequent”
        else
                if( yearly count > 4)
                        modFreq = do 1year
                else if(yearly count == 4)
                        modFreq = “Few times yearly”
                else                                                    //yearly count < 4
                        modFreq = “Infrequent”
    Return modFreq
Stop
1 year: Start
    modFreq
    yearly count = count pw changes within last 1 year
        if (yearly count <10)
                modFreq = “Few times yearly”
        else                                                    //more than 10 times in the past 1 year
                ten month count = count pw changes within last 10 months
                if (ten month count < yearly count)
                        modFreq = do 10months
                else
                        modFreq = “Recent activity”
    Return modFreq
Stop
10months: Start
    modFreq
    eight month count = count pw changes within last 8 months
    Read ten month count
        If (eight month count < ten month count)
                modFreq = do 8months
        else
                modFreq = “Recent activity”
    Return modFreq
Stop
8months: Start
    modFreq
    six month count = count pw changes within last 6 months
    Read eight month count
        If (six month count < eight month count)
                modFreq = do 6months
        else
                modFreq = “Recent activity”
    Return modFreq
Stop
6months: Start
    modFreq
    four month count = count pw changes within last 4 months
    Read six month count
        If (four month count < six month count)
                modFreq = do 4months
        else
                modFreq = “Recent activity”
    Return modFreq
Stop
4months: Start
    modFreq
    two month count = count pw changes within last 2 months
    Read four month count
        If (two month count < four month count)
                modFreq = do 2months
        else
                modFreq = “Recent activity”
    Return modFreq
```

Algorithm

```
Stop
2months: Start
    modFreq
    monthly count = count pw changes within last 1 month
    Read two month count
        If (monthly count < two month count)
            modFreq = do 1month
        else
            modFreq = “Recent activity”
    Return modFreq
Stop
1month: Start
    modFreq
    Read monthly count
        If (monthly count < 2)
            modFreq = “Monthly”
        else                                                    //more than once a month
            two week count = count pw changes within last 14 days
            if (two week count < monthly count)
                modFreq = do 2weeks
            else
                modFreq = “Recent activity”
    Return modFreq
Stop
Two weeks: Start
    modFreq
    Read two week count
        If (two week count <2)
            modFreq = “Every 2 weeks”
        else                                                    //more than once every 2 weeks
            weekly count = count pw changes within last 7 days
            if (weekly count < two week count)
                if (weekly count < 2)
                    modFreq = “Weekly”
                else                                            //more than once a week
                    modFreq = “Excessively
            else                                                //weekly count is the same as two week count
                modFreq = “Recent activity”
    Return modFreq
 Stop
```

Table B.2 – Algorithm for Calculating Password Reuse

Algorithm

```
Start
    pwReuse
    Read employee data
        Total pws = number of passwords in past 1 year
        Reused_1_2 = number of passwords reused Once or Twice in past 1 year
        Reused_3_5 = number of passwords reused 3, 4 or 5 times in past 1 year
        Reused_6_9 = number of passwords reused 6, 7, 8 or 9 times in past 1 year
        Reused_10up = number of passwords reused 10 times or more in past 1 year
        pwReuse = total pws+_+reused_10up+_+reused_6_9+_+reused_3_5+_+reused_1_2
    Return pwReuse
Stop
```

Table B.3 – Reused Algorithm for Calculating Password Strength

Algorithm

```
Start
    Strength value
    PW strength
    Read password
        If (there are lower class characters)
            Strength value += 25
        If (there are upper class characters)
            Strength value +=25
        If (there are digits)
            Strength value +=25
        If (there are symbols)
            Strength value +=25
    Read strength value
        If (strength value == 100)
            PW strength = “Strong”
        If (strength value == 75)
            PW strength = “Medium”
        If (strength value == 50)
            PW strength = “Weak”
        If (strength value == 25)
            PW strength = “Very weak”
    Return PW strength
Stop
```

Table B.4 – Algorithm for Calculating Data Backup Frequency

Algorithm

```
Start
    buFreq
    Read employee’s backup data
        monthly count = number of backups during past 1 month
        total bu = total number of backups since joining organization
            if (total bu <= monthly count)                          //Joined less than 1 month ago
                buFreq = “Too new to determine”
            else
                if (monthly count < 4)
                    buFreq = “Infrequent”
                else                                                //more than 4 backups per month
                    weekly count = number of backups during the past 7 days
                    if (weekly count < 2)
                        buFreq = “Weekly”
                    else                                            //more than once a week
                        daily count = number of backups during the past 1 day
                        if (daily count < weekly count)
                            if (daily count < 2)
                                buFreq = “Daily”
                            else                                    //more than once a day
                                buFreq = “Excessive”
                        else                                        //daily count is same as weekly count
                            buFreq = “Recent activity”
    Return buFreq
Stop
```

Table B.5 – Algorithms for Calculating Unauthorized Data Access and Attempted Backing Up of Unauthorized Data

Algorithm

```
Data Access: Start
    Accessing over clearance
    Accessing without need to know
    objClassification
    empClearance
    Read classification of selected data object
        If (classification == "Public")
            objClassification = 5
        else if (classification == "Unclassified")
            objClassification = 4
        else if (classification == "Classified")
            objClassification = 3
        else if (classification == "Secret")
            objClassification = 2
        else                                                    //classification == "Top Secret"
            objClassification = 1
    Read selected project
    Read employee's project
    Read employee's clearance level
        If (clearance == "Top Secret")
            empClearance = 1
        else If (clearance == "Secret")
            empClearance = 2
        else If (clearance == "Classified")
            empClearance = 3
        else If (clearance == "Unclassified")
            empClearance = 4
        else                                                    //clearance == "Public"
            empClearance = 5
    Read employee's current accessing over clearance
    Read employee's current accessing without need to know
    if (empClearance <= objClassification)          //employee has same or higher clearance than the data
        if (employee's project == selected project)                  //employee has need to know
            Open file
        Else                                          //same or higher clearance, but no need to know
            Accessing without need to know = current accessing without need to know + 1
            Not authorized to access file
    Else                                                                        //lower clearance
        Accessing over clearance = current over clearance + 1
        If (employee's project == selected project)          //lower clearance but has need to know
            Not authorized to access file
        Else                                                 //lower clearance and no need to know
            Accessing without need to know = current accessing without need to know + 1
            Not authorized to access file
Stop
Data Backup: Start
    Accessing over clearance
    Accessing without need to know
    Backup count
    objClassification
    empClearance
    Read classification of selected data object
        If (classification == "Public")
            objClassification = 5
        else if (classification == "Unclassified")
            objClassification = 4
        else if (classification == "Classified")
            objClassification = 3
        else if (classification == "Secret")
            objClassification = 2
```

Algorithm

```
        else                                                    //classification == "Top Secret"
            objClassification = 1
    Read selected project
    Read employee's project
    Read employee's clearance level
        If (clearance == "Top Secret")
            empClearance = 1
        else If (clearance == "Secret")
            empClearance = 2
        else If (clearance == "Classified")
            empClearance = 3
        else If (clearance == "Unclassified")
            empClearance = 4
        else                                                    //clearance == "Public"
            empClearance = 5
    Read employee's current accessing over clearance
    Read employee's current accessing without need to know
    if (empClearance <= objClassification)                      //employee has same or higher clearance than the data
        if (employee's project == selected project)             //employee has need to know
            Backup count += 1
            Backup file
        Else                                                    //same or higher clearance, but no need to know
            Accessing without need to know = current accessing without need to know + 1
            Not authorized to backup file
    Else                                                        //lower clearance
        Accessing over clearance = current over clearance + 1
        If (employee's project == selected project)             //lower clearance but has need to know
            Not authorized to backup file
        Else                                                    //lower clearance and no need to know
            Accessing without need to know = current accessing without need to know + 1
            Not authorized to backup file
Stop
```

Table B.6 – Summarized Algorithm for Compiling Security Behavioural Profiles

Algorithm

```
Start
  words
  words_mgrView
  words_secperView
  words_bginfo
  words_cyber
  status
  unauthorized access potential
  improper sharing potential
  motive
  security status
  introverted
  extraverted
  sensing
  intuitive
  thinking
  feeling
  judging
  perceiving
  IE
  SN
  TF
  JP
  personality type
  behavioural profile
  Read manager's view
      if( manager's view contains "forget" or "Forget")
          if( manager's view contains "not forget" or Not forget")          //Does not forget keycards
              if( words does not contain "Security conscious")
                  Read security rule configuration for "Not Forgetting Keycards & PINs" (Security conscious, Information
revealed easily, Understands and values ISM rules, Sociable, Ambitious, Has technical knowledge about computers, Easy
hack target, Suspicious behaviour, May have social incentives, May have career-wise incentives, May have personal
motives, May have financial motives, May have psychological motives and potential, Potential for improper sharing,
Potential for unauthorized access, Minimum acceptable number)
                  ConfigureBhvRulesMgr
                  thinking++
          else                                                              //Forgets keycards
              if( words does not contain "Not security conscious")
                  ConfigureBhvRulesMgr
              improper sharing potential = true
……
  behavioural profile = words appended to each other
  if( behavioural profile contains "motive" or "incentive")
      motive = true
  if( unauthorized access potential is true)
      add "Has potential for unauthorized access" to status
  if( improper sharing potential is true)
      add "Has potential for improper information sharing" to status
  if( motive is true)
      add "Has motives/incentives" to status
  security status = status appended to each other
  if ( introverted > extraverted)
      IE = "I"
  else if( introverted < extraverted)
      IE = "E"
  Else
      IE = "?"
  if ( sensing > intuitive)
      SN = "S"
  else if( sensing < intuitive)
      SN = "N"
  Else
```

Algorithm

```
        SN = “?”
   if ( thinking > feeling)
        TF = “T”
   else if( thinking < feeling)
        TF = “F”
   Else
        TF = “?”
   if ( judging > perceiving)
        JP = “J”
   else if( judging < perceiving)
        JP = “P”
   Else
        JP = “?”
   Personality type = IE + SN + TF + JP
   if (personality type is “ISTJ” or “ISFJ” or “INFJ” or “INTJ” or “ISTP” or “ISFP” or “INFP” or “INTP” or “ESTP” or
“ESFP” or “ENFP” or “ENTP” or “ESTJ” or “ESFJ” or “ENFJ” or ENTJ”)
        write personality traits obtained from MBTI to each personality type
   else
        write “Cannot determine personality”
Stop
ConfigureBhvRulesMgr: Start
        if(item1 is not "-")
            if(item1 is"Y" or item1 is"y")
               if(words does not contain "Security conscious")
                     Security conscious++
               if(words_mgrView does not contain "Security conscious")
                        Security conscious++
            else if(item1 is"N" or item1 is "n")
               if(words does not contain "Not security conscious")
                     Not security conscious++
               if(words_mgrView does not contain "Not security conscious")
                     Not security conscious++
……
Stop
```

Table B.7 – Algorithm for Computing Security Training Schedules

Algorithm

```
Start
  all schedules
  segments
  random schedule
  workshop schedule
  seminar schedule
  inspection schedule
  today's date
  Read current random schedule, current workshop schedule, current seminar schedule, current inspection schedule
      if( current random schedule is after today's date)
            use current random schedule as random schedule
      if( current workshop schedule is after today's date)
            use current workshop schedule as workshop schedule
      if( current seminar schedule is after today's date)
            use current seminar schedule as seminar schedule
      if( current inspection schedule is after today's date)
            use current inspection schedule as inspection schedule
      if( all available schedules are in the past)
            all schedules = do Compute training schedules
            split all schedules into segments
            random schedule = segment[0]
            workshop schedule = segment[1]
            seminar schedule = segment[2]
            inspection schedule = segment[3]
  Update database with new training schedules
  Colour selected date for random schedule green
  if( workshop schedule is not "None")
      colour selected date for workshop schedule blue
  if( seminar schedule is not "None")
      colour selected date for seminar schedule red
  if( inspection schedule is not "None")
      colour selected date for inspection schedule yellow
Stop
Compute training schedules:  Start
  random schedule
  workshop schedule
  seminar schedule
  inspection schedule
  schedules
  today's day
  days to add
      days to add = number of days from last Tuesday
      random schedule = days to add + 28                                  //4 weeks from coming Tuesday
      Read security status
            if( security status contains "sharing")
                  workshop schedule = days to add + 1 + 14              //2 weeks from coming Wednesday
            if( security status contains "unauthorized")
                  seminar schedule = days to add + 1 + 7                //1 week from coming Wednesday
            if( security status contains = "motive")
                  inspection schedule = days to add + 2 + 14            //2 weeks from coming Thursday
      schedules = random schedule + "_" + workshop schedule + "_" + seminar schedule + "_" + inspection schedule
  Return schedules
Stop
```

Appendix C – Usability Evaluation Survey & Results

Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns – Usability Evaluation: Group A (Tabular Data)

Assuming you are the Information Security Officer of a business organization, please follow the instructions given below to compile security behavioural profiles and training schedules for as many employees as possible in order to answer the attached questionnaire.

A. Given below is information gathered by the Security Behavioural Profiling System about employees' cyber activities on 2013 September 30th. Please use this information to **find the behavioural patterns** for the given employees.

1. **Password security behaviour** – use the given "Password Changes" tables (tables 1-10) of the last twelve months until 2013 September 30th along with the "Employee" table (table 11) to find:

i. Password Strength – strength of the current password (password with the latest date)

ii. Password Modifying Frequency:

a) Infrequent
b) Few times a year
c) Monthly
d) Every 2 weeks
e) Weekly
f) Excessively
g) Recent activity – if password modification occurred at a slower rate, but has suddenly picked up pace
h) Too new to determine – if the employee joined the organization less than a month before 2013 September 30th, this may be ignored

iii. Password Reuse:

a) Ten times or over
b) Six-to-nine times
c) Three-to-five times
d) One-to-two times – , this may be ignored since this is not considered a security infraction

2. **Data backup behaviour** – use the given "Data Backup" tables (tables 12-21) of the last few months until 2013 September 30th along with the "Employee" table (table 11) to find:

iv. Data Backup Frequency:

a) Infrequent
b) Weekly
c) Daily
d) Excessive
e) Recent activity – if the password modification occurred at a slower rate, but has suddenly picked up pace
f) Too new to determine – if the employee joined the organization less than a month before 2013 September 30th, this may be ignored

3. **Data access behaviour** – use the given "Data Access" tables (tables 22-31) of the employees since their time of joining the organization until 2013 September 30th to find the number of attempts to access data without authorization:

v. Over clearance level – if the classification level of the data object is higher than the clearance level of the employee according to the list below (where the highest level is denoted by 1 and the lowest level is denoted by 5):
    1) Top secret
    2) Secret
    3) Classified
    4) Unclassified
    5) Public

vi. Without Need-to-Know – if the project the employee is working on is different to the project the data object belongs to (employee's project ID is different to the data object's project ID)

B. Use the partial results of employees' cyber activities calculated above together with the background information of the employees ("Background Information" table – table 32) and the personal observations about their security behaviour inputted by their managers and security personnel ("Personal Views" table – table 33) given below, to **compile the security behavioural profiles** for these employees using the "Default Rules for Computing Security Behavioural Characteristics" table (table 34) below. In the "Default Rules for Computing Security Behavioural Characteristics" table, "N" depicts not having the corresponding characteristic, while "Y" depicts having that characteristic. The characteristics not relevant to a corresponding observable behaviour are coloured in grey. Thus, according to the default values, the security behavioural profile for an employee who leaves items unattended, for example, will contain the characteristics of not being security conscious, easily revealing information, not valuing or understanding ISM rules, and having a potential for improper sharing of information. The number column shows the maximum acceptable value before the relevant field is considered. Thus, if more than 1 password is reused 'three-to-five times', or if any passwords are reused 'six-to-nine' times, or 'ten times or over', the security behavioural profile for that employee will contain the characteristics of not being security conscious, not valuing or understanding ISM rules, being an easy hack target, and having a potential for improper sharing of information.

C. Use the security behavioural profiles compiled above to **determine and schedule the security education and training to be given** to these employees according to the following rules:

Assuming there are no security trainings currently scheduled,

- For all employees → a random periodic risk perception renewal (automatic pop-up security awareness presentation followed by a Q&A session) scheduled in 4 weeks from the coming Tuesday
- For employees who have a potential for improper information sharing → a hands-on security workshop (conducted by external security professionals) scheduled in 2 weeks from the coming Wednesday
- For employees who have a potential for unauthorized access to information → a security seminar (conducted by security managers and legal officials) scheduled in a week from the coming Wednesday

- For employees who are deemed to have any kind of motive or incentive for engaging in improper information sharing or unauthorized access → closer inspection including background checks (by security managers and human resource managers) scheduled in 2 weeks from the coming Thursday

For example, the training schedules computed on 30th September 2013 for an employee who requires all four types of security training will include: a random awareness training on Tuesday, 29th October 2013, a security workshop on Wednesday, 16th October 2013, a security seminar on Wednesday, 9th October 2013, and a security inspection on Thursday, 17th October 2013.

Table 1 – Password Changes of Emp0001

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
cAt00lHm	2012-10-01	Medium	emp0001
0lLLah0l	2012-10-26	Medium	emp0001
cAt00lHm	2012-11-01	Medium	emp0001
0lLLah0l	2012-12-02	Medium	emp0001
cAt00lHm	2012-12-28	Medium	emp0001
pme20001	2013-01-02	Weak	emp0001
0lLLah0l	2013-02-01	Medium	emp0001
cAt00lHm	2013-02-22	Medium	emp0001
aBc0Ma01	2013-03-17	Medium	emp0001
cAt00lHm	2013-04-03	Medium	emp0001
pme20001	2013-04-26	Weak	emp0001
aBc0Ma01	2013-05-13	Medium	emp0001
aBc0Ma01	2013-06-28	Medium	emp0001
aBc0Ma01	2013-07-26	Medium	emp0001
cAt00lHm	2013-08-08	Medium	emp0001
abc00001	2013-08-22	Weak	emp0001
cAt00lHm	2013-09-06	Medium	emp0001
HmT2la03	2013-09-22	Medium	emp0001

Table 2 – Password Changes of Emp0002

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
02mW0a02	2012-11-30	Medium	emp0002
02mW0a02	2013-01-25	Medium	emp0002
pme00002	2013-03-14	Weak	emp0002
wHm0 a02	2013-05-21	Medium	emp0002
02mW0a02	2013-07-20	Medium	emp0002
wHm0 a02	2013-08-02	Medium	emp0002
bbb00002	2013-08-23	Weak	emp0002
pme20002	2013-08-30	Weak	emp0002
02mW0a02	2013-09-06	Medium	emp0002
wHm0 a02	2013-09-13	Medium	emp0002
Am020wHt	2013-09-22	Medium	emp0002
Hw020Am	2013-09-30	Medium	emp0002

Table 3 – Password Changes of Emp0003

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
pme00003	2013-02-01	Weak	emp0003
pme00003	2013-03-17	Weak	emp0003
eee00003	2013-04-13	Weak	emp0003
ccc00003	2013-05-13	Weak	emp0003
abc00003	2013-06-20	Weak	emp0003
pme00003	2013-07-15	Weak	emp0003
abc00003	2013-08-20	Weak	emp0003
ccc00003	2013-09-06	Weak	emp0003
abc00003	2013-09-13	Weak	emp0003
ccc00003	2013-09-19	Weak	emp0003
abc00003	2013-09-20	Weak	emp0003
sm03ills	2013-09-23	Weak	emp0003
abc00003	2013-09-24	Weak	emp0003
eee00003	2013-09-25	Weak	emp0003
abc00003	2013-09-26	Weak	emp0003
pme00003	2013-09-26	Weak	emp0003
abc00003	2013-09-27	Weak	emp0003
pme00003	2013-09-28	Weak	emp0003
abc00003	2013-09-28	Weak	emp0003
sm03ills	2013-09-30	Weak	emp0003

Table 4 – Password Changes of Emp0004

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
dk#%2lL3	2012-11-20	Strong	emp0004
90dJl%kl	2013-01-17	Strong	emp0004
fL43&jH4	2013-03-14	Strong	emp0004
e89#)dk3	2013-04-19	Strong	emp0004
dj*kL032	2013-05-20	Strong	emp0004
d87J$kl4	2013-06-22	Strong	emp0004
sE4jF#03	2013-07-02	Strong	emp0004
sJ%9io87	2013-07-16	Strong	emp0004
fL43&jH4	2013-07-29	Strong	emp0004
d8&9kHdH	2013-08-12	Strong	emp0004
gh89Km0J	2013-08-27	Medium	emp0004
Fj400lYn	2013-09-09	Medium	emp0004
3nY%f$4J	2013-09-23	Strong	emp0004

Table 5 – Password Changes of Emp0005

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
cLj015a5	2013-03-09	Medium	emp0005
jC55all0	2013-06-05	Medium	emp0005
Llc55jAb	2013-09-23	Medium	emp0005

Table 6 – Password Changes of Emp0006

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
emp0006	2013-03-09	Weak	emp0006
feL6$ks2	2013-03-14	Strong	emp0006
sFl2j(k2	2013-04-12	Strong	emp0006
fSt62s6^	2013-05-24	Strong	emp0006
LeT6s2F0	2013-06-28	Medium	emp0006
hTi66Af	2013-07-26	Medium	emp0006
RaL66sT	2013-08-22	Medium	emp0006
%Ts6hF06	2013-09-30	Strong	emp0006

Table 7 – Password Changes of Emp0007

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
4cMc7LrI	2013-04-02	Medium	emp0007
LcM7cC0l	2013-04-26	Medium	emp0007
RaI007lC	2013-05-31	Medium	emp0007
LcM7cC0l	2013-06-28	Medium	emp0007
cL7MM92c	2013-07-19	Medium	emp0007
LcM7cC0l	2013-08-22	Medium	emp0007
cCmC7k05	2013-09-23	Medium	emp0007

Table 8 – Password Changes of Emp0008

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
emp0008	2013-05-13	Weak	emp0008
scolt888	2013-09-23	Weak	emp0008

Table 9 – Password Changes of Emp0009

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
fLd9Gav9	2012-10-22	Medium	emp0009
gAv99FlD	2013-04-16	Medium	emp0009
gFields9	2013-06-10	Medium	emp0009
fGv09ilD	2013-07-18	Medium	emp0009
gAv99FlD	2013-08-30	Medium	emp0009
fLd9Gav9	2013-09-02	Medium	emp0009
fLd9Gav9	2013-09-11	Medium	emp0009
fGv09ilD	2013-09-17	Medium	emp0009
gAv99FlD	2013-09-20	Medium	emp0009
Vg9dL0iF	2013-09-23	Medium	emp0009
fGv09ilD	2013-09-24	Medium	emp0009
fLd9Gav9	2013-09-25	Medium	emp0009
gAv99FlD	2013-09-26	Medium	emp0009
fGv09ilD	2013-09-27	Medium	emp0009
gAv99FlD	2013-09-28	Medium	emp0009
fLd9Gav9	2013-09-28	Medium	emp0009
gFields9	2013-09-30	Medium	emp0009
Vg9dL0iF	2013-09-30	Medium	emp0009

Table 10 – Password Changes of Emp0010

pwchngs_pw character va	pwchngs_date date	pwchngs_strength character varying(	pwchngs_empid character varyir
emp0010	2013-09-02	Weak	emp0010
sAm10RaH	2013-09-05	Medium	emp0010
Am#aH10s	2013-09-23	Strong	emp0010

Table 11 – Employee

emp_id characte	emp_joineddate date
emp0001	2010-01-01
emp0002	2011-01-01
emp0003	2013-02-01
emp0004	2010-01-01
emp0005	2013-03-09
emp0006	2013-03-09
emp0007	2013-04-02
emp0008	2013-05-13
emp0009	2009-10-01
emp0010	2013-09-02

Table 12 – Data Backup by Emp0001

dbu_emp_id character va	dbu_date date
emp0001	2013-08-23
emp0001	2013-08-27
emp0001	2013-08-29
emp0001	2013-08-30
emp0001	2013-08-31
emp0001	2013-09-02
emp0001	2013-09-03
emp0001	2013-09-04
emp0001	2013-09-06
emp0001	2013-09-09
emp0001	2013-09-10
emp0001	2013-09-12
emp0001	2013-09-13
emp0001	2013-09-17
emp0001	2013-09-18
emp0001	2013-09-20
emp0001	2013-09-21
emp0001	2013-09-22
emp0001	2013-09-24
emp0001	2013-09-26
emp0001	2013-09-27
emp0001	2013-09-30

Table 13 – Data Backup by Emp0002

dbu_emp_id character va	dbu_date date
emp0002	2013-08-23
emp0002	2013-08-23
emp0002	2013-08-23
emp0002	2013-08-27
emp0002	2013-08-30
emp0002	2013-08-30
emp0002	2013-09-04
emp0002	2013-09-06
emp0002	2013-09-09
emp0002	2013-09-09
emp0002	2013-09-11
emp0002	2013-09-11
emp0002	2013-09-13
emp0002	2013-09-13
emp0002	2013-09-13
emp0002	2013-09-17
emp0002	2013-09-19
emp0002	2013-09-19
emp0002	2013-09-20
emp0002	2013-09-20
emp0002	2013-09-22
emp0002	2013-09-22
emp0002	2013-09-24
emp0002	2013-09-24
emp0002	2013-09-25
emp0002	2013-09-26
emp0002	2013-09-27
emp0002	2013-09-27
emp0002	2013-09-27
emp0002	2013-09-30
emp0002	2013-09-30

Table 14 – Data Backup by Emp0003

dbu_emp_id character va	dbu_date date
emp0003	2013-08-12
emp0003	2013-08-16
emp0003	2013-08-26
emp0003	2013-08-30
emp0003	2013-09-03
emp0003	2013-09-06
emp0003	2013-09-10
emp0003	2013-09-10
emp0003	2013-09-10
emp0003	2013-09-12
emp0003	2013-09-13
emp0003	2013-09-13
emp0003	2013-09-18
emp0003	2013-09-18
emp0003	2013-09-19
emp0003	2013-09-20
emp0003	2013-09-20
emp0003	2013-09-22
emp0003	2013-09-22
emp0003	2013-09-22
emp0003	2013-09-24
emp0003	2013-09-25
emp0003	2013-09-26
emp0003	2013-09-26
emp0003	2013-09-27
emp0003	2013-09-27
emp0003	2013-09-30
emp0003	2013-09-30

Table 15 – Data Backup by Emp0004

dbu_emp_id character va	dbu_date date
emp0004	2013-08-19
emp0004	2013-08-26
emp0004	2013-08-31
emp0004	2013-09-02
emp0004	2013-09-06
emp0004	2013-09-09
emp0004	2013-09-14
emp0004	2013-09-22
emp0004	2013-09-30

Table 16 – Data Backup by Emp0005

dbu_emp_id character va	dbu_date date
emp0005	2013-04-01
emp0005	2013-05-13
emp0005	2013-07-31
emp0005	2013-08-20
emp0005	2013-09-22

Table 17 – Data Backup by Emp0006

dbu_emp_id character va	dbu_date date
emp0006	2013-08-23
emp0006	2013-08-27
emp0006	2013-08-30
emp0006	2013-09-02
emp0006	2013-09-03
emp0006	2013-09-04
emp0006	2013-09-06
emp0006	2013-09-09
emp0006	2013-09-10
emp0006	2013-09-12
emp0006	2013-09-13
emp0006	2013-09-18
emp0006	2013-09-19
emp0006	2013-09-20
emp0006	2013-09-22
emp0006	2013-09-24
emp0006	2013-09-26
emp0006	2013-09-30

Table 18 – Data Backup by Emp0007

dbu_emp_id character va	dbu_date date
emp0007	2013-08-26
emp0007	2013-09-02
emp0007	2013-09-09
emp0007	2013-09-15
emp0007	2013-09-22
emp0007	2013-09-30

Table 19 – Data Backup by Emp0008

dbu_emp_id character va	dbu_date date
emp0008	2013-05-13
emp0008	2013-07-26
emp0008	2013-08-30
emp0008	2013-09-22

Table 20 – Data Backup by Emp0009

dbu_emp_id character va	dbu_date date
emp0009	2013-03-22
emp0009	2013-04-26
emp0009	2013-05-24
emp0009	2013-06-28
emp0009	2013-07-22
emp0009	2013-08-23
emp0009	2013-09-06
emp0009	2013-09-06
emp0009	2013-09-09
emp0009	2013-09-13
emp0009	2013-09-22
emp0009	2013-09-22
emp0009	2013-09-22
emp0009	2013-09-22
emp0009	2013-09-30
emp0009	2013-09-30
emp0009	2013-09-30
emp0009	2013-09-30
emp0009	2013-09-30
emp0009	2013-09-30

Table 21 – Data Backup by Emp0010

dbu_emp_id character va	dbu_date date
emp0010	2013-09-06
emp0010	2013-09-13
emp0010	2013-09-22
emp0010	2013-09-30

Table 22 – Data Access by Emp0001

empda_c characte	empda_ characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-08-31
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0001	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30

Table 23 – Data Access by Emp0002

empda_ characte	empda_e characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0001	emp0002	Classified	Classified	Retrieve	proj0001	proj0001	2013-06-01
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-06-01
obj0003	emp0002	Classified	Classified	Retrieve	proj0001	proj0003	2013-06-01
obj0002	emp0002	Unclassif	Classified	BackUp	proj0001	proj0002	2013-06-01
obj0004	emp0002	Classified	Classified	Retrieve	proj0001	proj0002	2013-06-01
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0002	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30

Table 24 – Data Access by Emp0003

empda_c characte	empda_ characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0002	emp0003	Unclassif	Unclassif	Retrieve	proj0002	proj0002	2013-08-31
obj0004	emp0003	Classified	Unclassif	Retrieve	proj0002	proj0002	2013-08-31
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30
obj0002	emp0003	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-30

Table 25 – Data Access by Emp0004

empda_c characte	empda_ characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-08-31
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0004	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30

Table 26 – Data Access by Emp0005

empda_c characte	empda_ characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0004	emp0005	Classified	Unclassif	Retrieve	proj0002	proj0002	2013-08-30
obj0002	emp0005	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0005	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0005	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22

Table 27 – Data Access by Emp0006

empda_c characte	empda_e characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0001	emp0006	Classified	Classified	Retrieve	proj0001	proj0001	2013-08-31
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30
obj0001	emp0006	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30

Table 28 – Data Access by Emp0007

empda_c characte	empda_e characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0001	emp0007	Classified	Classified	Retrieve	proj0003	proj0001	2013-08-31
obj0003	emp0007	Classified	Classified	Retrieve	proj0003	proj0003	2013-08-31
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0007	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30

Table 29 – Data Access by Emp0008

empda_o characte	empda_e character	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_pro character varyir	empda_acce date
obj0002	emp0008	Unclassif	Unclassif	Retrieve	proj0002	proj0002	2013-08-31
obj0002	emp0008	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0008	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0002	emp0008	Unclassif	Unclassif	BackUp	proj0002	proj0002	2013-09-22
obj0003	emp0008	Classified	Unclassif	Retrieve	proj0002	proj0003	2013-09-30

Table 30 – Data Access by Emp0009

empda_o character	empda_e character	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_pro character varyir	empda_acce date
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-22
obj0005	emp0009	Secret	Classified	Retrieve	proj0003	proj0004	2013-09-27
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30
obj0003	emp0009	Classified	Classified	BackUp	proj0003	proj0003	2013-09-30

Table 31 – Data Access by Emp0010

empda_c characte	empda_e characte	empda_objclassification character varying(10)	empda_empclearance character varying(10)	empda_ty character	empda_emp_proj character varying	empda_obj_proj character varyin	empda_acce date
obj0004	emp0010	Classified	Classified	Retrieve	proj0001	proj0002	2013-09-22
obj0001	emp0010	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0010	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0010	Classified	Classified	BackUp	proj0001	proj0001	2013-09-22
obj0001	emp0010	Classified	Classified	BackUp	proj0001	proj0001	2013-09-30

Table 32 – Background Information

empbg_e character	empbg_maritalstatus character varying(10)	empbg_dependents integer	empbg_accrecord character varying(200)	empbg_finstatusrec character varying(200)	empbg_crimrec character varying(200)
emp0001	Unmarried	0	BA in Accounting	Steady income since 2010	None
emp0002	Married	1	BS in Computer Science	Steady income since 2006	None
emp0003	Divorced	1	Computer Tech Certification	Low income	Juvenile breaking and entering
emp0004	Widowed	2	MS in Computer Engineering	Steady income since 2008	Teenaged hacking into Federal Database
emp0005	Married	3	Computer Tech Certification	Low income	None
emp0006	Divorced	1	MS in Computer Engineering	Steady Income since 2013	None
emp0007	Unmarried	0	BA in Accounting	Steady income since 2007	None
emp0008	Unmarried	1	Computer Tech Certification	Low income	Juvenile shoplifting
emp0009	Divorced	3	BA in Accounting	Steady income since 2010	None
emp0010	Married	2	MS in Computer Engineering	Steady income since 2013	None

Table 33 – Personal Views

empbhv_id character va	empbhv_managerview character varying(100)	empbhv_secpersonnelview character varying(100)
empbhv0001	Forgets keycards	Leaves items unattended
empbhv0002	Sociable, ambitious	
empbhv0003	Writes passwords on stickynotes, leaves items unattended	Forgets keycards
empbhv0004	Security conscious, ambitious	
empbhv0005	Sociable, lends keycards and pins	Forgets keycards
empbhv0006	Security conscious, understands and values ISM rules, ambitious	
empbhv0007	Lends keycards and pins, does not value ISM rules	
empbhv0008	Lends keycards and pins, does not understand or value ISM rules	Lends keycards and pins, writes passwords on stickynotes
empbhv0009	Ambitious	
empbhv0010		

Table 34 – Default Rules for Computing Security Behavioural Characteristics

Activity	**Security Conscious**	**Reveals Information**	**Values / Understands ISM Rules**	**Sociable**	**Ambitious**	**Technical Knowledge**	**Easy Hack Target**	**Suspicious Behaviour**	**Social Incentive**	**Career-wise Incentive**	**Personal Motive**	**Financial Motive**	**Psychological Motive**	**Improper Sharing Potential**	**Unauthorized Access Potential**	**Number**
Personally Observed Non-Cyber Activities																
Forgets keys	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not forget keys	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Leaves items unattended	N	Y	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not leave items	Y	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Sociable	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	
Not sociable	-	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	
Ambitious	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	Y	
Not ambitious	-	-	-	-	N	-	-	-	-	-	-	-	-	-	-	
Writes down passwords	N	Y	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Does not write passwords	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Lends keys/PINs	-	Y	-	-	-	-	-	-	Y	-	-	-	-	Y	-	
Does not lend keys/PINs	-	N	-	-	-	-	-	-	-	-	-	-	-	-	-	
Security conscious	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Not security conscious	N	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
Understands/values ISM rules	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	
Does not understand /value ISM rules	-	-	N	-	-	-	-	-	-	-	-	-	-	Y	-	
Background Information – Marital Status, Dependents, Academic Record, Financial Status, Criminal Record																
Married									-	-	-	-	-	Y	-	
Unmarried									Y	-	-	-	-	-	-	
Divorced									-	-	Y	-	-	-	-	
Widowed									-	-	-	-	-	-	-	
Dependents												Y				2
BS/MS in Computers						Y									Y	
No BA/BS/MS									Y							
Low income												Y				
Has criminal record													Y		Y	
Cyber Activities – Password Strength																
Very weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Weak	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	
Medium	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Strong	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Cyber Activities – Password Modification Frequency																
Infrequent	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Few times a year	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	
Monthly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Every 2 weeks	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	Y	
Cyber Activities – Password Reuse																
Ten times or over	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Six-to-nine times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	0
Three-to-five times	N	-	N	-	-	-	Y	-	-	-	-	-	-	Y	-	1
Cyber Activities – Attempts to Access Data without Authorization																
Over clearance	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
No need-to-know	-	-	N	-	-	-	-	Y	-	-	-	-	-	-	Y	0
Cyber Activities – Backup Frequency																
Infrequent	N	-	N	-	-	-	-	-	-	-	-	-	-	-	-	
Weekly	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Daily	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Excessively	-	-	-	-	Y	-	-	Y	-	-	-	-	-	Y	-	
Recent activity	-	-	-	-	-	-	-	Y	-	-	-	-	-	Y	-	

Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns – Usability Evaluation: Group B (Textual Results)

Assuming you are the Information Security Officer of a business organization, please follow the instructions given below to view security behavioural profiles and compute training schedules for as many employees as possible in order to answer the attached questionnaire.

A. Log in to the system using the following details:
   User ID: iso0001
   Password: osi00001

   Select task: View Security Behavioural Profiles and click "OK"

   View summarized profile: Select employee from drop-down list and click "Request Behavioural Profiles"

   View detailed profile: click "View Details"

   Request separate views: click "Separate Views"

B. Use the security behavioural profiles viewed above to **determine and schedule the security education and training to be given** to these employees according to the following rules:

Assuming there are no security trainings currently scheduled,

- For all employees → a random periodic risk perception renewal (automatic pop-up security awareness presentation followed by a Q&A session) scheduled in 4 weeks from the coming Tuesday
- For employees who have a potential for improper information sharing → a hands-on security workshop (conducted by external security professionals) scheduled in 2 weeks from the coming Wednesday
- For employees who have a potential for unauthorized access to information → a security seminar (conducted by security managers and legal officials) scheduled in a week from the coming Wednesday
- For employees who are deemed to have any kind of motive or incentive for engaging in improper information sharing or unauthorized access → closer inspection including background checks (by security managers and human resource managers) scheduled in 2 weeks from the coming Thursday

For example, the training schedules computed on 30th September 2013 for an employee who requires all four types of security training will include: a random awareness training on Tuesday, 29th October 2013, a security workshop on Wednesday, 16th October 2013, a security seminar on Wednesday, 9th October 2013, and a security inspection on Thursday, 17th October 2013.

Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns – Usability Evaluation: Group C (Graphical Results)

Assuming you are the Information Security Officer of a business organization, please follow the instructions given below to view security behavioural profiles and training schedules for as many employees as possible in order to answer the attached questionnaire.

A. Log in to the system using the following details:
   User ID: iso0001
   Password: osi00001

   Select task: View Security Behavioural Profiles and click “OK”

   Select employee from drop-down list and click “Request Behavioural Profiles”

   View graphical profile: click “View Graphs”

   View training schedules: click “View Training Schedules”

Usability Evaluation Questionnaire

Nationality - _____

Residing country - _____

Occupation - _____

1	The speed with which you were able to arrive at decisions concerning the security behaviour of employees:	Very fast	Fast	Moderate	Slow	Very slow
2	The speed with which you were able to schedule security training programmes for employees:	Very fast	Fast	Moderate	Slow	Very slow
3	The amount of computations/calculations required to determine the security behaviour of the employees:	Extensive	Large	Moderate	Small	Very small
4	The amount of computations/calculations required to determine the security training schedules for the employees:	Extensive	Large	Moderate	Small	Very small
5	Additional tools/applications needed or preferred for arriving at conclusions:	(e.g.: stationery/ database management system/ spreadsheet application/ computer program)				
6	Presentation of the (raw) data given:	Very high	High	Moderate	Poor	Very poor
7	The extent/scope of detail gathered from the (raw) data presented to you:	Highly detailed	Moderately detailed	Comprehensive	Summarized/ concise	Highly summarized
8	The usefulness of (raw) data presented to you in determining the potential for information security infractions by employees:	Very high	High	Average	Low	Very low
9	Ease of determining the potential and/or motives of the employees for improper information sharing and/or unauthorized data access:	Very easy	Easy	Not easy	Difficult	Very difficult
10	Ease of recognizing any personal bias the managers or security personnel might have towards the employees:	Very easy	Easy	Not easy	Difficult	Very difficult
11	The overall usability of the system given to you:	Very high	High	Average	Low	Very low
12	Additional Comments:					

Thank you.

-Suchinthi Fernando (3rd Year Doctoral Student – Information Science & Control Engineering, Nagaoka University of Technology)